

INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL
Programa de Pós-graduação em Propriedade Intelectual e Inovação
Mestrado Profissional em Propriedade Intelectual e Inovação

Gitana de Moura Viana

**“LI E CONCORDO”: UMA ANÁLISE DA PERFILIZAÇÃO NAS REDES SOCIAIS
DA META PLATFORM INC À LUZ DO ART 2º DA LEI GERAL DE PROTEÇÃO
DE DADOS**

Rio de Janeiro

2025

Gitana de Moura Viana

**“LI E CONCORDO”: UMA ANÁLISE DA PERFILIZAÇÃO NAS REDES SOCIAIS
DA META PLATFORM INC À LUZ DO ART 2º DA LEI GERAL DE PROTEÇÃO
DE DADOS**

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Pós-graduação em Propriedade Intelectual e Inovação, do Instituto Nacional da Propriedade Industrial.

Orientador: Prof. Dr. Leandro Miranda Malavota

Rio de Janeiro

2025

V614g VIANA, Gitana de Moura

“Li e concordo”: uma análise da perfilização nas redes sociais da Meta Platform Inc à luz do art. 2º da Lei Geral de Proteção de Dados / Gitana de Moura Viana. – Rio de Janeiro, 2025.

144 f.

Dissertação (Mestrado em Propriedade Intelectual e Inovação) - Instituto Nacional da Propriedade Industrial, 2025.

1. Defesa do Consumidor.
 2. Profiling.
 3. Proteção de Dados.
 4. Direitos Fundamentais.
 5. Meta Platforms Inc.
- I. Instituto Nacional da Propriedade Industrial, Rio de Janeiro. II. Título.

CDD: 347.77

Autorizo, apenas para fins acadêmicos e científicos, a reprodução total ou parcial desta dissertação, desde que citada a fonte.

Assinatura

Data

Gitana de Moura Viana

**“LI E CONCORDO”: UMA ANÁLISE DA PERFILIZAÇÃO NAS REDES SOCIAIS
DA META PLATFORM INC À LUZ DO ART 2º DA LEI GERAL DE PROTEÇÃO
DE DADOS**

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Pós-graduação em Propriedade Intelectual e Inovação, do Instituto Nacional da Propriedade Industrial.

Aprovada em ____ de ____ de ____.

Banca Examinadora:

Prof. Dr. Leandro Miranda Malavota (Orientador)
Instituto Nacional da Propriedade Industrial

Vinicius Bogéa
Instituto Nacional de Propriedade Industrial (INPI)

Lucas Ruiz Balconi
Universidade de São Paulo (USP)

Evanildo Vieira dos Santos
Instituto Nacional de Propriedade Industrial (INPI)

Rio de Janeiro
2025

AGRADECIMENTOS

Este trabalho nasce da quebra de uma crença limitante, de um diálogo interno em que me permiti acreditar que poderia mais, que eu poderia alçar novos voos. Eu fiz a minha parte, mas não cheguei aqui sozinha. Agradeço à minha família e aos amigos, especialmente ao meu pai, Otavio Viana, por acreditar em mim de forma incondicional e me fazer ver a vida de uma forma mais leve.

Agradeço ao meu orientador, Leandro Malavota, pela paciência e empatia dedicadas ao longo desses anos, sempre assertivo e otimista, e aos professores do programa, que nos ensinam com tanta dedicação e amor pelo ofício. Vocês são uma inspiração de profissionais que eu desejo ser.

Foi de extrema importância para mim, conhecer e conviver com pessoas inspiradoras. Aproveito este momento para agradecer aos profissionais que me incentivaram a participar do processo seletivo: Wilson Lima, Bruno Candido, Mariana Moretti, Letícia Fiuza e tantos outros que vibraram comigo neste sonho. A excelência de vocês me impulsiona a estar em constante evolução.

Agradeço também a todos os negros que vieram antes de mim, abrindo portas e caminhos para que este momento fosse possível. Este não é apenas um título de mestre, é a continuidade de um legado, do qual eu faço parte, mas que é muito maior do que eu.

RESUMO

VIANA, Gitana de Moura. **“Li e concordo”: uma análise da perfilização nas redes sociais da Meta Platform Inc à luz do art. 2º da Lei Geral de Proteção de Dados.** 2025. 144 f. Dissertação (Mestrado em Propriedade Intelectual e Inovação) – Instituto Nacional da Propriedade Industrial, Rio de Janeiro. 2025.

A presente dissertação analisa a prática de *profiling* nas redes sociais da Meta Platforms Inc. (Facebook e Instagram), sob a perspectiva dos princípios do livre desenvolvimento da personalidade e da autodeterminação informativa, previstos no artigo 2º da Lei Geral de Proteção de Dados (LGPD). A partir de abordagem qualitativa e análise documental, investiga-se a compatibilidade dessa técnica com o arcabouço jurídico-normativo brasileiro. O estudo utiliza a teoria da identidade narrativa como parâmetro para compreender de que forma os processos algorítmicos interferem na construção da identidade dos usuários, especialmente no contexto brasileiro, marcado por vulnerabilidade técnica, assimetria informacional e dependência digital. Conclui-se que o consentimento, isoladamente, é insuficiente para assegurar a proteção efetiva dos direitos fundamentais, sendo necessária a adoção de medidas regulatórias capazes de equilibrar o desenvolvimento tecnológico com a salvaguarda da personalidade e da soberania informacional.

Palavras-chave: Defesa do Consumidor. *Profiling*. Proteção de dados. Redes sociais. Meta Platforms Inc. Direitos Fundamentais.

ABSTRACT

VIANA, Gitana de Moura. **“Li e concordo”: uma análise da perfilização nas redes sociais da Meta Platform Inc à luz do art. 2º da Lei Geral de Proteção de Dados.** 2025. 144 f. Dissertação (Mestrado em Propriedade Intelectual e Inovação) – Instituto Nacional da Propriedade Industrial, Rio de Janeiro. 2025.

This dissertation analyzes the practice of profiling on the social networks of Meta Platforms Inc. (Facebook and Instagram), from the perspective of the principles of the free development of personality and informational self-determination, as provided in Article 2 of the Brazilian General Data Protection Law (LGPD). Using a qualitative approach and documentary analysis, it investigates the compatibility of this technique with the Brazilian legal and regulatory framework. The study adopts the theory of narrative identity as a parameter to understand how algorithmic processes interfere with the construction of users' identities, especially with in the Brazilian context, marked by technical vulnerability, informational asymmetry, and digital dependency. The conclusion is that consent, by itself, is insufficient to ensure the effective protection of fundamental rights, making it necessary to adopt regulatory measures capable of balancing technological development with the safeguarding of personality and informational sovereignty.

Keywords: Consumer Protection. Profile. Data Protection. Social Networks. Meta Platforms Inc. .Fundamental Rights.

SUMÁRIO

| | | |
|-------|---------------------------------------------------------------------------------------------------------------------------|----|
| 1 | INTRODUÇÃO | 9 |
| 1.1 | Contextualização e Relevância do Tema | 9 |
| 1.2 | Objetivos | 16 |
| 1.2.1 | Objetivo Geral | 16 |
| 1.2.2 | Objetivos Específicos | 16 |
| 1.3 | Justificativa | 16 |
| 1.4 | Método de pesquisa | 20 |
| 1.5 | Questão de pesquisa | 20 |
| 1.6 | Hipótese | 20 |
| 1.7 | Referenciais teóricos | 21 |
| 2 | CONSTRUÇÃO JURÍDICA NORMATIVA DAS LEIS DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL | 26 |
| 2.1 | Privacidade e Proteção de Dados na Constituição Federal, previsão jurídica e evolução do instituto | 26 |
| 2.2 | Código de Defesa do Consumidor (CDC)..... | 30 |
| 2.3 | Marco Civil da Internet | 37 |
| 2.4 | O consentimento como base legal para <i>profiling</i>..... | 40 |
| 2.4.1 | Consentimento e a Lacuna jurídica | 45 |
| 2.5 | Lei Geral de Proteção de Dados | 47 |
| 2.6 | O papel da Agência Nacional de Proteção de dados – ANPD | 54 |
| 3 | O LIVRE DESENVOLVIMENTO DA PERSONALIDADE E A AUTODETERMINAÇÃO INFORMATIVA NA PROTEÇÃO DE DADOS..... | 59 |
| 3.1 | Precedentes históricos sobre direito ao livre desenvolvimento da personalidade e autodeterminação informativa..... | 59 |
| 3.1.1 | O Julgamento da Lei do Censo de 1983..... | 59 |
| 3.1.2 | O Caso IBGE..... | 62 |
| 3.2 | A personalidade como um direito fundamental | 64 |
| 3.3 | O Direito ao Livre Desenvolvimento da Personalidade - privacidade e proteção de dados nas redes sociais | 67 |

SUMÁRIO (continuação)

| | | |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 3.4 | Redes sociais, <i>profiling</i> e identidade | 71 |
| 3.4.1 | <i>Profiling</i> como fato social..... | 71 |
| 3.4.2 | <i>Profiling</i> e identidade | 72 |
| 3.5 | A narrativa líquida: uma intersecção entre os conceitos de modernidade líquida de Zygmunt Bauman e a identidade narrativa de Paul Ricoeur aplicados ao profiling | 80 |
| 4 | A ERA DA INFORMAÇÃO – ECONOMIA DE VIGILÂNCIA, DATIFICAÇÃO DA VIDA E SEUS IMPACTOS NO COMPORTAMENTO HUMANO | 84 |
| 4.1 | O que é Profiling? Classificação no Tratamento Automatizado de Dados | 84 |
| 4.2 | Breve histórico da formação da empresa Meta Platform Inc | 88 |
| 4.3 | Google e o legado do superávit comportamental..... | 92 |
| 4.4 | O Capitalismo de Vigilância | 95 |
| 4.4.1 | Capitalismo de vigilância e o livre desenvolvimento da personalidade | 99 |
| 5 | DESAFIOS GLOBAIS E PERSPECTIVAS REGULATÓRIAS DO PROFILING EM REDES SOCIAIS..... | 102 |
| 5.1 | O caso Cambridge Analytica..... | 102 |
| 5.2 | Colonialismo de dados e o monopólio GAFAM..... | 105 |
| 5.3 | Harmonização jurídica internacional, soberania digital e desafios globais da proteção de dados..... | 111 |
| 5.4 | O devido processo informacional e horizontalidade de direitos fundamentais..... | 114 |
| 6 | INICIATIVAS DE REEQUILÍBRIO DE INTERESSES..... | 117 |
| 6.1 | Direito a Inferências Razoáveis..... | 117 |
| 6.2 | Transparência na era do profiling: o papel dos relatórios de impacto..... | 120 |
| 6.3 | Iniciativas legislativas e a insuficiência normativa frente à perfilização automatizada | 122 |
| 6.3.1 | Projeto de Lei 2.630/2020/ PL das Fake News | 122 |
| 6.3.2 | Projetos sobre inteligência artificial e a omissão sobre perfilização | 123 |
| 6.4 | Reavaliação do Consentimento e Propostas de Solução para o <i>Profiling</i> em | |

| | | |
|----------|---------------------------|------------|
| 7 | Redes Sociais..... | 124 |
| | CONCLUSÃO | 130 |
| | REFERÊNCIAS | 134 |

1 INTRODUÇÃO

A popularização da internet e a incorporação das redes sociais no cotidiano da população brasileira transformaram significativamente a maneira como as pessoas interagem e compartilham suas experiências sociais, que passam a ser digitalizadas e todo o comportamento, individual ou coletivo, neste ambiente é transformado em informação (Susanto; Meiryani, 2019).

A importância da pesquisa está em analisar a prática de *profiling*¹ enquanto técnica base de um modelo de negócio, posicionando as redes sociais da Meta Platform Inc. como parte de uma engrenagem maior, qual seja a economia da informação, mas que se destaca por ter sido incorporada na rotina dos usuários, que dedicam parte significativa de seu tempo na utilização dos aplicativos da empresa.

1.1 Contextualização e Relevância do Tema

Diante das diversas possibilidades de utilização dos dados, a pesquisa opta por demonstrar o potencial de interferência do *profiling*, ou perfilização, aqui tratados como sinônimos, comportamento do consumidor/usuário e a possibilidade da técnica em interferir no livre desenvolvimento da personalidade e na autodeterminação informativa dos usuários no ambiente das redes sociais Facebook e Instagram, e a partir desta observação expandir a aplicação em uma escala maior.

Profiling pode ser definido como o processo de coleta, análise e interpretação de dados dos usuários para a construção de perfis detalhados, que representam suas características, comportamentos e interesses, criados a partir das interações realizadas na plataforma. Com base nesses dados, algoritmos identificam padrões e tendências de comportamento, permitindo diversas aplicações, como a personalização de campanhas publicitárias e recomendações automatizadas de conteúdo (Silva *et al.*, 2025).

Em uma sociedade hiper conectada as redes sociais desempenham um papel central na economia digital contemporânea, utilizando da técnica de *profiling* para coletar, processar e analisar dados dos usuários. Essas plataformas operam como peças fundamentais na

¹ Perfilização (*profiling*): É a técnica de análise massiva de dados para criar perfis detalhados dos usuários.

engrenagem da economia da informação. Extrapolando a finalidade de otimização de vendas e/ou experiência do consumidor, mas permitindo uma verdadeira datificação da vida humana.²

Esse acúmulo de informações levanta diversas preocupações como, privacidade, proteção de dados, e as interferências dessa datificação no desenvolvimento da personalidade e autodeterminação informativa, direitos estes previstos nas normas brasileiras, em especial na Lei Geral de Proteção de Dados (LGPD), diploma específico sobre proteção de dados no Brasil.

Ocorre que, geralmente a legislação não é capaz de acompanhar os avanços tecnológicos em tempo real, necessitando ser revisitada à luz do momento atual, para averiguar se os comandos da lei são capazes de regular determinada prática e cumprir a finalidade para o qual foi criada, sendo este o objetivo ao qual o trabalho se dispõe.

Apresentadas a contextualização e relevância do tema, apresentaremos os assuntos de forma introdutória de forma a conectar as ideias que em conjunto formam o objeto da pesquisa. iniciando por uma breve exposição dos marcadores históricos da economia até chegarmos no monto atual, qual seja a economia informacional, sendo este o período em que este trabalho se situa.

Ao longo da história, a humanidade vivenciou distintas formas de organização social e econômica, cada qual marcada por elementos centrais que definiram seus marcos históricos. O desenvolvimento econômico pode ser compreendido a partir de três grandes eras: agrícola, industrial e informacional (Bioni, 2019).

Na era agrícola, a terra e os recursos naturais renováveis constituíam os principais ativos econômicos, sendo a produção voltada majoritariamente para o consumo próprio, com predomínio da força de trabalho manual e do escambo como forma de comércio (Bioni, 2019).

Com a Revolução Industrial, a partir do século XVIII, a introdução das máquinas e o uso de fontes de energia como carvão e petróleo permitiram a produção em larga escala, promovendo a concentração de ativos em recursos não renováveis e a expansão dos mercados industriais (Bioni, 2019).

² Datificação é o processo de transformar aspectos variados da vida social, econômica e individual em dados quantificáveis e digitalizáveis, permitindo seu monitoramento, análise e utilização por meio de tecnologias digitais. Esse fenômeno, intensificado com o avanço das Tecnologias da Informação e Comunicação, consiste na coleta, armazenamento e análise massiva de informações sobre comportamentos, interações e eventos cotidianos, convertendo-os em formatos que podem ser processados por sistemas computacionais. A datificação, assim, fundamenta práticas como big data, o monitoramento em tempo real e a análise preditiva, impactando setores como economia, trabalho, consumo e governança social.

A partir da segunda metade do século XX, consolida-se a economia da informação, caracterizada pela centralidade da ciência, da tecnologia e da informação na produção, pela flexibilidade e reorganização dos processos produtivos, e pela formação de redes globais que articulam fluxos de informação em tempo real. Nessa nova era, a informação torna-se a matéria-prima fundamental, e a capacidade de processá-la e aplicá-la define a produtividade e a competitividade de empresas, regiões e países.

O paradigma informacional, como destaca Castells, implica uma lógica de redes, flexibilidade estrutural e integração global, transformando profundamente as relações econômicas, sociais e culturais (Castells, 2020).

Na economia da informação, o ativo central são os dados, tendo o comportamento humano como principal fonte de extração. Normalmente realizada a partir de uma dinâmica monetização por dados, a empresa permite o acesso gratuito ao serviço e o usuário fornece seus dados como moeda de troca. Com o tempo tais tecnologias passam a fazer parte do cotidiano, neste momento se instala uma estrutura coletora de dados (Silveira; Souza e Cassino, 2021).

Setores como tecnologia, finanças, saúde e educação exemplificam a centralidade da informação. Plataformas digitais e redes sociais extraem e analisam grandes volumes de dados para direcionar publicidade e aprimorar algoritmos de recomendação. No mercado financeiro, informações em tempo real orientam investimentos e operações automatizadas. Na saúde, prontuários eletrônicos e sistemas de inteligência artificial otimizam diagnósticos e tratamentos. Na educação, a análise de dados permite personalizar o ensino e monitorar o desempenho dos estudantes, transformando práticas pedagógicas tradicionais.

Em *O colonialismo de dados*, Silveira, Souza e Cassino (2021) explicam que assim como outras formas de extração, como o petróleo, que exigiu plataformas de perfuração para que fossem possíveis de retirada, os dados demandam infraestruturas tecnológicas como *data centers*, *cookies*, algoritmos para coleta, processamento e monetização, assim o avanço tecnológico permitiu a montagem dessa estrutura de datificação da vida .

A título de exemplo, sobre como os dados de interação do consumidor são utilizados para a criação e otimização de produtos, temos o caso da empresa Amazon que desenvolveu e patenteou uma tecnologia inovadora chamada *anticipatory shipping* (entrega antecipada), que utiliza inteligência artificial e análise preditiva de dados para antecipar o envio de produtos aos clientes antes mesmo da finalização da compra (Poechhacker; Nyckel, 2020)

O sistema opera por meio do cruzamento de informações do usuário como histórico de buscas, frequência de acesso a páginas de produtos, tempo de permanência nessas páginas, listas de desejos, e a partir dessas informações calcula a probabilidade de um consumidor efetuar determinada compra. Quando essa probabilidade é considerada alta, o produto é enviado do centro de distribuição para um *hub* logístico próximo ao cliente em potencial, o que possibilita uma redução significativa no tempo de entrega, e maior eficiência em logística da empresa (Poechhacker; Nyckel, 2020)

Traçando um paralelo entre ativo predominante x fonte de extração dos marcos econômicos, percebe-se que, na era agrícola o ativo se extraía da terra; na era industrial de fontes energética no solo e/ou subsolo. Na economia da informação o ativo é extraído de pessoas, consumidores finais ou não, suas interações preferências, localização, sem uma limitação objetiva, de modo que tudo pode ser um dado capaz de trazer alguma informação, o ser humano passa a ser a fonte de coleta, e consequentemente o meio para obtenção de lucro o que em tese viola o princípio da dignidade da pessoa humana.

Nesse contexto, este estudo se propõe a responder se a prática de *profiling* é compatível com os princípios do livre desenvolvimento e da autodeterminação informativa, fundamentos do artigo 2º da Lei Geral de Proteção de Dados, para entender como as redes sociais da empresa meta tem impactado os diferentes aspectos dos direitos de personalidade dos indivíduos. O objetivo é discutir os desdobramentos da técnica sob uma perspectiva que abrange não apenas os interesses individuais, mas também coletivos, a fim de responder se a Lei Geral de Proteção de Dados³ cumpre, de modo eficaz, a finalidade de proteção da individualidade do usuário entendendo que a privacidade, o livre desenvolvimento da personalidade e a autodeterminação são esferas da personalidade dos usuários.

Considerando a multiplicidade de ambientes em que esses dados podem ser captados, optou-se por estudar a prática no contexto das redes sociais da empresa Meta Platforms Inc. avançando no estudo da técnica ao aplicar a discussão contemporânea sobre a influência da tecnologia no desenvolvimento humano, escolhendo uma tecnologia específica, *profiling*, em um ambiente específico, as redes sociais da empresa Meta Inc.

A escolha desse recorte se justifica pela expressiva adesão dos usuários brasileiros aos aplicativos da empresa, Facebook e Instagram, o que faz do Brasil a terceira maior população consumidora dessas redes sociais no mundo, atrás apenas de Índia e China (Pacete, 2023). A

³ Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - Mediante o fornecimento de consentimento pelo titular;

pesquisa busca entender os efeitos colaterais decorrentes da coleta intensiva e constante de dados feita pela empresa.

O foco da análise recai sobre a capacidade ou não da LGPD em garantir que a perfilização feita pelas redes sociais estejam alinhadas com os fundamentos para o qual a lei foi criada. Para isso serão analisadas pesquisas recentes sobre como as redes sociais têm influenciado na formação da personalidade e comportamento dos usuários, para ao fim responder se a legislação apontada é suficiente ou não para disciplinar o tema.

Busca-se compreender se a perfilização é uma prática compatível com o princípio do fundamento da personalidade. Além disso, discute-se se, mesmo diante do consentimento do usuário, é necessária uma atuação mais efetiva do Estado como regulador das relações entre usuários e redes sociais, considerando que a privacidade e proteção de dados pessoais integra os direitos de personalidade e compõe o rol de direitos fundamentais previstos no art. 5º, LXXIX, da Constituição Federal de 1988⁴.

Contudo, os direitos dos usuários não são o único bem a ser considerado, sendo de suma importância a ponderação entre o direito à livre iniciativa e o incentivo ao desenvolvimento tecnológico no país. Diante disso, estudar a proteção de dados no contexto das redes sociais torna-se essencial para compreender e equilibrar os múltiplos direitos previstos na legislação brasileira, direitos estes que não se anulam e precisam coexistir de forma harmoniosa.

Danilo Doneda destaca a necessidade de uma releitura do direito à privacidade à luz das transformações sociais atuais, a fim de garantir sua efetividade. Tal atualização é fundamental para que o Estado possa atuar de maneira eficaz, considerando o novo contexto em que a privacidade se insere, sob pena de se instaurar um estado de não direito e abrir espaço para mecanismos sociais alheios aos valores estatais (Doneda, 2006).

Considerando a necessidade de harmonização mencionada e o desequilíbrio presumido de forças na relação entre usuário/consumidor e fornecedor, a segunda seção do trabalho será dedicado à construção jurídico-normativa sobre privacidade e proteção de dados no Brasil, evidenciando a construção jurídico/normativa sobre o tema.

Não há na legislação brasileira qualquer vedação para o fornecimento de dados pessoais, bem como para o seu tratamento por empresas privadas, o que por consequência permite considerar a prática legítima, desde que realizada nos termos do art. 7º da LGPD, que

⁴ LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

indica as bases legais para o tratamento de dados por empresas privadas, porém, tal artigo deve ser analisado em conjunto com outros dispositivos, que visam garantir a efetividade da proteção, como os direitos de autodeterminação informativa e livre desenvolvimento humano. Temas que serão aprofundados na terceira seção.

Como destacado por Mendes (2014), a análise da proteção de dados pessoais na sociedade da informação tem a função de compreender e responder aos desafios sociais, ressaltando que o problema não reside na tecnologia, nas inovações ou na rede social em si, mas nas decisões tomadas em relação a elas e no equilíbrio de interesses dos atores envolvidos.

Diante das particularidades do tratamento massivo de dados e de suas implicações coletivas, este trabalho reserva um momento específico para discutir os principais atores envolvidos nesse debate, com destaque para as grandes empresas de tecnologia, conhecidas como *Big Techs*, Google, Apple, Facebook, Amazon e Microsoft, tradicionalmente agrupadas sob a sigla GAFAM.

A proposta de dedicar uma seção exclusiva às *Big Techs* visa analisar o viés político do mercado de dados, abordando a informação como ativo de manutenção de poder e o movimento cíclico do capitalismo, que periodicamente se reorganiza para criar estruturas de domínio global, neste trabalho caracterizado pelo acúmulo de informações por um pequeno grupo de empresas norte-americanas em um contexto que pode, inclusive, colocar o Brasil novamente na posição de fornecedor de *commodities*, agora na forma de dados.

Ressalta-se que o estudo não questiona os benefícios e ônus das redes sociais nem propõe a proibição do tratamento de dados por empresas privadas fornecedoras do serviço, mas visa destacar aspectos jurídicos e políticos específicos do tema.

O cerne da reflexão é questionar os limites dessa prática à luz da legislação sobre proteção de dados, considerar as particularidades políticas e sociais do Brasil no contexto da economia da informação⁵. A pesquisa reconhece a autonomia da vontade das partes, mas relativiza tal autonomia por se tratar de uma relação de consumo, e consequentemente uma parte vulnerável, conforme será abordado em item próprio.

⁵ Concepção no qual o conhecimento é considerado um insumo para o processo produtivo moderno. Uma economia baseada no conhecimento se apoia efetivamente na habilidade de gerar, armazenar, recuperar, processar e transmitir informações, funções potencialmente aplicáveis a todas as atividades humanas (Tigre. 2005 p 24-25).

A Seção 2 abordará a construção normativa da privacidade e proteção de dados no Brasil, destacando como as transformações sociais, especialmente no ambiente digital, exigiram a adaptação de normas existentes e a criação de novas regulamentações.

Serão discutidas as dificuldades de regular modelos tecnológicos em um cenário onde as legislações não acompanham a velocidade das inovações. Entre os fatores responsáveis por essa defasagem estão a incompreensão das nuances tecnológicas, a burocracia legislativa e pressões de interesses econômicos, o que pode resultar em normas inadequadas à realidade (Rossi, 2023).

A proposta da segunda seção é realizar um balanço jurídico, mapeando como o ordenamento brasileiro se estruturou para a era da informação. Em seguida, o texto questionará como a legislação brasileira pode ser aplicada para disciplinar a prática de *profiling* no ambiente das redes sociais da empresa Meta.Inc para ao fim demonstrar nos resultados se, do ponto de vista material, existe uma ponderação entre o direito de livre iniciativa da empresa Meta os direitos de autodeterminação informativa e o livre desenvolvimento humano dos usuários.

A Seção 3 analisa os direitos ao livre desenvolvimento da personalidade, articulando-os à prática de perfilização algorítmica e parte da articulação desses direitos com a teoria da identidade narrativa de Paul Ricoeur, discutindo como a coleta massiva de dados e a intervenção do algoritmo de perfilização pode afetar a construção da identidade e a autonomia dos usuários.

A Seção 4 investiga a presença das redes sociais da Meta Platforms Inc. na economia da informação, com foco na realidade brasileira. A partir da forte adesão dos usuários às plataformas, analisa-se a posição do Brasil no mercado global de dados e os riscos de dependência tecnológica e neocolonialismo informacional.

A Seção 5 aprofunda os desafios regulatórios do profiling, destacando o caso Cambridge Analytica e o papel da Meta. Platform Inc. no contexto das big techs. e a fragilidade do uso do consentimento como base legal para a permissão da perfilização.

A Seção 6 apresenta as conclusões da pesquisa, retomando os objetivos, discutindo a insuficiência do consentimento como base legal e destacando os achados do trabalho. Aponta as contribuições teóricas e práticas, reconhece limitações e propõe direções para estudos futuros sobre regulação de dados. Finalizando a pesquisa serão postas as conclusões, respondendo se os objetivos aqui propostos foram devidamente alcançados, as limitações metodológicas da pesquisa e as perspectivas de continuidade do objeto analisado.

1.2 Objetivos

Os objetivos da pesquisa são organizados em geral e em específicos, a seguir.

1.2.1 Objetivo Geral

Analisar a compatibilidade da técnica de *profiling* praticada nas redes sociais da Meta Platforms Inc. (Instagram e Facebook) com o princípio do livre desenvolvimento da personalidade e da autodeterminação informativa do artigo art. 2º da Lei Geral de Proteção de Dados - LGPD para entender se há ou não violação destes princípios.

1.2.2 Objetivos Específicos

1. Mapear o arcabouço jurídico-normativo brasileiro sobre privacidade e proteção de dados, incluindo:
2. Avaliar a função e os limites do consentimento como base legal para o profiling, considerando o desequilíbrio de poder entre usuários e plataformas (modelo *take it or leave it*).
3. Investigar o modelo de negócio da Meta Platforms Inc. e sua relação com princípios como inviolabilidade da vida privada (CF, Art. 5º, X), livre desenvolvimento humano e autodeterminação informativa.
4. Levantar as principais discussões sobre o tema.

1.3 Justificativa

Das novas possibilidades trazidas pela tecnológica, a exemplo das redes sociais, surgem também novas problemáticas como a digitalização⁶, datificação da vida⁷, racismo

⁶ O termo *digitalização* refere-se à conversão de práticas sociais, econômicas e comunicacionais para formatos digitais, processo que, segundo Castells (2009), é parte da reestruturação informacional do capitalismo e influencia diretamente a organização da vida em rede.

⁷ A expressão *datificação da vida* designa a transformação de aspectos cotidianos da experiência humana em dados passíveis de coleta, análise e exploração econômica. Conforme Zuboff (2021), trata-se da conversão da experiência em comportamento previsto e comercializado por sistemas de inteligência algorítmica.

algorítmico⁸ entre outras. O que inicialmente era apenas uma ferramenta para interação de universitários, cresceu e se desenvolveu ao ponto de ser utilizada por parte significativa da população mundial, com utilização que vai muito além de interação e entretenimento.

Além de um local de interação as redes sociais permitiram que se instalassem um novo modelo de negócios, em especial a publicidade segmentada, que permite encurtar o caminho entre produto/serviço do e consumidor final, a partir da identificação do perfil de consumo de cada usuário.

E como ponto central desta engrenagem estão os dados, capturados, processados e agrupados de forma a conhecer este usuário consumidor e oferecer produtos com base em seus gostos, técnica conhecida como *profiling*. Entretanto esta técnica tem chamado a atenção, de diversas áreas como a sociologia, a política e o direito, que têm questionado quais os impactos desta prática nos consumidores/usuários, e entre tais questionamentos está a influência dessa perfilização no comportamento humano e a capacidade de afetação do livre desenvolvimento da personalidade e da autodeterminação informativa, que é o objeto desta pesquisa.

A chamada “indústria de dados” já é considerada uma das principais forças econômicas do século XXI, sendo os dados pessoais frequentemente referidos como “o novo petróleo” (The World’s, 2017). Diferentemente das commodities tradicionais, os dados possuem uso praticamente ilimitado, ampliando o potencial de lucro das empresas a custos marginais reduzidos. O comportamento dos usuários nas redes sociais, é transformado em um ativo imaterial de altíssimo valor, a informação deixa de ser meio e passa a ser o próprio produto comercializado.

Historicamente, países colonizadores, como Estados Unidos, consolidaram vantagens estruturais, pois acumularam capital, tecnologia e poder decisório, estabelecendo padrões que outros países tendem a seguir ou se adaptar, enquanto países colonizados ou periféricos, como o Brasil, permanecem em posição subordinada, reproduzindo padrões de dependência e exportação de matéria prima, que a economia da informação é representada pelos dados, cujo valor agregado é apropriado pelos centros hegemônicos.

Ainda atualmente, o Brasil exporta em sua maioria, produtos de baixa densidade tecnológica, como soja petróleo bruto e minério de ferro, que apresentam baixo grau de

⁸O conceito de *racismo algorítmico* descreve a reprodução de vieses e discriminações raciais em sistemas automatizados. Noble (2022) analisa como mecanismos de busca e tecnologias digitais refletem e amplificam desigualdades sociais existentes, consolidando práticas discriminatórias sob aparição de neutralidade.

processamento industrial, sendo seu preço determinado principalmente pela demanda internacional e não pela incorporação de tecnologia ou inovação (Righi; Santos; Oliveira, 2021).

Pesquisa realizada pelo Instituto de Estudos para Desenvolvimento Intelectual (IEDI), entre 1995 e 2021 (último dado disponível), mostram que no que se refere ao índice de complexidade econômica (ICE), o Brasil tem demonstrado uma piora significativa no ranking mundial de complexidade, saindo da 25º posição em 1995, para 70º posição em 2021 (IEDI, 2024)⁹. Tais dados são relevantes para entender que o atraso tecnológico e a permanência do Brasil enquanto fornecedor de *commodities*, afeta o país em diversos setores, em uma movimentação macro, todavia, para que não se desvie do objeto não exploraremos aqui as causas do atraso tecnológico que afetou pais nas últimas décadas.

No contexto digital, o país repete esse padrão ao exportar dados de seus cidadãos, enquanto o processamento e a monetização desses dados ocorrem majoritariamente em empresas estrangeiras, como a Meta Platforms Inc. O que cria uma assimetria de poder e conhecimento, reforçando a dependência tecnológica do Brasil em relação a países desenvolvidos e grandes plataformas digitais no mercado de dados (Pacete, 2023).

Na estrutura da economia informacional, as redes sociais desempenham papel crucial na coleta, processamento e monetização de dados, muitas vezes sem que os usuários compreendam plenamente a finalidade e o impacto desse tratamento. Segundo relatório do Data Reportal (2025), o Brasil contava com 144 milhões de identidades ativas em redes sociais em janeiro de 2025, o que representa cerca de 67,8% da população total. O país é reconhecido como um dos maiores mercados de redes sociais do mundo, com o Instagram entre as plataformas mais populares, somando mais de 141 milhões de usuários ativos em setembro de 2024.

Entender o comportamento dos consumidores que permite que as empresas fornecedoras possam otimizar seus produtos/serviços e torná-los cada vez mais competitivos, o que a princípio não seria um problema, porém a ausência de um controle eficaz sobre o tratamento dos dados pode afetar não só a privacidade individual, mas também direitos

⁹ O Índice de Complexidade Econômica (ICE) é uma medida da sofisticação produtiva de um país, baseada na análise da sua estrutura exportadora. Segundo o IEDI, o ICE combina informações sobre a diversidade da economia (quantidade de produtos exportados) e a ubiquidade desses produtos (quanto países também os exportam). Economias mais complexas são aquelas que apresentam uma pauta exportadora diversificada e exportam produtos sofisticados, com baixa ubiquidade, ou seja, que poucos países conseguem produzir e exportar. Já economias menos complexas tendem a exportar produtos mais comuns e menos exigentes em capacidades técnicas e tecnológicas (IEDI, 2024).

difusos e interesses coletivos, dada a escala e o impacto social dessas práticas (Righi; Santos; Oliveira, 2021).

Casos emblemáticos, como o Cambridge Analytica, em 2018, demonstram como o uso indevido de dados pode influenciar processos políticos e sociais, extrapolando o âmbito individual e exigindo respostas regulatórias robustas (Silva, 2024; Zuboff, 2019). O caso Cambridge Analítica é apenas um dos muitos exemplos em que dados de milhões de usuários foram coletados sem consentimento para criar perfis psicológicos e direcionar campanhas políticas.

Outras implicações evidenciam o poder da empresa Meta em modular condutas e opiniões, como a estratégia de algoritmos e design de plataformas, que são projetados para capturar a atenção dos usuários e maximizar o tempo de uso, especialmente entre jovens. Recursos como rolagem infinita, notificações constantes e filtros de beleza, desenvolvidos para promover engajamento compulsivo e dependência, impactando a saúde mental e a autoimagem de adolescentes (Chagas et al., 2025).

Nesta lógica, um processamento inadequado pode gerar desdobramentos públicos e privados, justificando a intervenção estatal para proteger direitos fundamentais e coletivos, mesmo diante do consentimento formal dos titulares (Brasil, 2018).

O tema merece ser estudado pela sua relevância teórica, prática e social, propondo uma discussão atual sobre proteção de dados. O impacto sobre parcela expressiva da sociedade torna a matéria simultaneamente um direito individual e coletivo (Hoffmann-Riem, 1997 *apud* Mendes, 2014, p. 610).

Diferentemente de estudos que abordam genericamente a proteção de dados ou os impactos das redes sociais, esta dissertação inova ao articular conceitos de direito, sociologia e filosofia para investigar como a perfilização automatizada pode afetar materialmente a autonomia dos usuários brasileiros, no contexto específico das redes sociais.

O trabalho avança o estado da arte ao propor uma reflexão sobre a suficiência do arcabouço normativo nacional, evidenciando lacunas regulatórias e sugerindo caminhos para uma regulação mais efetiva. O estudo também contribui ao incorporar o debate sobre colonialismo de dados, vulnerabilidade coletiva e soberania digital, ampliando o olhar para além da perspectiva individual e propondo a proteção de direitos difusos e coletivos frente ao poder das *big techs*. Dessa forma, a pesquisa não apenas preenche lacunas teóricas e normativas identificadas na literatura, mas também subsidia o desenvolvimento de políticas

públicas e estratégias regulatórias capazes de equilibrar inovação tecnológica e proteção dos direitos fundamentais no ambiente digital brasileiro.

1.4 Método de pesquisa

A pesquisa adota uma abordagem qualitativa de caráter indutivo, integrando análise documental para investigar a prática de *profiling* nas redes sociais Instagram e Facebook (Meta Platforms Inc.) sob a ótica do direito ao livre desenvolvimento da personalidade e autodeterminação informativa previsto na Lei Geral de Proteção de Dados (LGPD).

O método baseia-se na revisão crítica de fontes primárias, como legislação brasileira (Constituição Federal, LGPD, Marco Civil da Internet), diretrizes da Autoridade Nacional de Proteção de Dados (ANPD), termos de uso das plataformas, doutrinas afetas ao tema, e pesquisas sobre a influência das redes sociais no comportamento humano. Também serão utilizadas fontes secundárias, incluindo decisões judiciais recentes e relatórios de sanções administrativas aplicadas à empresa.

1.5 Questão de pesquisa

A prática de *profiling* nas redes sociais da Meta Platforms Inc, Facebook e Instagram, é compatível com os princípios fundamentais do livre desenvolvimento da personalidade e autodeterminação informativa previstos no art. 2º da Lei Geral de Proteção de Dados?

A pesquisa busca investigar, no contexto da legislação brasileira, se a perfilização dos usuários feita a partir da coleta de dados nas redes sociais da empresa Meta está materialmente de acordo com os princípios da LGPD.

1.6 Hipótese

A prática de *profiling* pela Meta Platforms Inc, mesmo quando fundamentada em consentimento formalmente válido, viola materialmente os direitos à autodeterminação informativa e ao livre desenvolvimento da personalidade previstos na Lei Geral de Proteção de Dados Brasileira .

A pesquisa parte do pressuposto de que a dinâmica atual de coleta e uso de dados em redes sociais para fins de *profiling* deveria ter como base legal o legítimo interesse da

empresa, de forma que não recaísse sobre o usuário a responsabilidade de decidir sobre o tratamento de seus dados, pois não possuiria expertise técnica para tal e por consequência, o arcabouço jurídico sobre o tema necessitaria de uma complementação normativa mais específica.

1.7 Referencial teórico

O referencial teórico estrutura-se em três eixos centrais, articulando debates sobre privacidade, assimetria informacional e capitalismo de vigilância, no contexto do *profiling* em redes sociais.

Com o avanço das tecnologias as instituições privadas perceberam os dados como um ativo econômico capaz de revolucionar produtos e processos, passando a captar dados para fins entender os desejos dos usuários e consequentemente ofertar produtos com maior assertividade, reduzindo custos de marketing e logística por exemplo.

Neste contexto a figura Orwelliana¹⁰ do *grande irmão*, representada pelo estado, passa a dividir espaço com o *pequeno irmão*, termo utilizado para se referir às empresas do setor privado que coletam, armazenam e processam dados de seus clientes, finais ou não, para atingir seus objetivos econômicos. (Buchner, 1999 citado por Shertell).

Shoshana Zuboff (2019), em sua obra *A era do capitalismo de vigilância, A lutar por um futuro humano na nova fronteira do poder*, analisa como o capitalismo contemporâneo transformou os dados pessoais em matéria-prima fundamental, configurando um novo modelo econômico baseado na extração, análise e comercialização de informações comportamentais.

Os referenciais foram pensados de modo a fundamentar o direito subjetivo dos usuários à privacidade, a prerrogativa destes de consentir ou não o tratamento de dados e a movimentação deste modelo de negócio como parte de uma engrenagem maior, uma reformulação do capitalismo e a lógica de controle, o chamado capitalismo de vigilância.

Zuboff descreve o capitalismo de vigilância como um sistema no qual grandes plataformas digitais, incluindo as redes da Meta Platform Inc. utilizam algoritmos para prever e influenciar o comportamento dos usuários, convertendo a experiência humana em mercadoria. Esse processo não apenas gera assimetrias de poder e conhecimento, mas também

¹⁰Adjetivo que se refere ao estilo, temas ou ideias presentes nas obras de George Orwell

ameaça a autonomia individual, ao manipular as escolhas e modelar identidades, comprometendo o livre desenvolvimento da personalidade e a autodeterminação informativa.

A contribuição de Zuboff é fundamental para compreender a dimensão estrutural do *profiling* e sua relação com a lógica econômica das redes sociais, oferecendo uma crítica à concentração de poder nas mãos de poucas empresas e à perda de controle dos indivíduos sobre seus próprios dados.

Danilo Doneda (2006), em sua obra *Da Privacidade à Proteção de Dados Pessoais*, questiona a noção tradicional de privacidade ao analisar como o avanço tecnológico e o tratamento massivo de dados desafiam os limites clássicos desse direito. O autor argumenta que a privacidade não pode ser compreendida apenas como o direito de estar só ou de proteger a intimidade, mas deve ser reinterpretada como uma garantia dinâmica, voltada à proteção do indivíduo frente aos novos riscos impostos pelo ambiente digital.

Doneda destaca que o controle sobre as informações pessoais é um elemento central da privacidade contemporânea, pois a capacidade de decidir sobre a circulação, o uso e a finalidade dos próprios dados configuram uma dimensão fundamental da autonomia individual.

Nesse sentido, o autor defende que a privacidade deve ser ressignificada como um direito à autodeterminação informativa, capaz de assegurar ao titular o poder de gerenciar e proteger suas informações pessoais diante das novas formas de vigilância e intervenção, tanto por parte do Estado quanto de empresas privadas, o que reflete diretamente sobre o livre desenvolvimento da personalidade e a dignidade humana em uma sociedade cada vez mais conectada (Doneda, 2006).

O Código Civil cuida dos direitos de personalidade no capítulo II dos artigos 11 a 21, garantindo os direitos voltados a resguardar a proteção da integridade corporal, o direito ao nome à imagem e à privacidade. Todavia, com as modificações sociais, a personalidade adquire novas perspectivas as quais naturalmente o Código Civil não pode alcançar ao tempo de sua edição, necessitando de uma reinterpretação para que possa alcançar a finalidade para o qual foi criado (Stancioli, 2011).

Sobre a interpretação ou reinterpretação do código civil sobre os direitos de personalidade traremos os precedentes jurisprudenciais do julgamento da lei do censo alemão e o caso IBGE, que figuraram como marcos históricos para o reconhecimento do livre desenvolvimento da personalidade e autodeterminação informativa como um direito.

Na análise das formalidades exigidas pela LGPD para que as redes sociais possam coletar os dados, utilizaremos os apontamentos feitos por Bruno Ricardo Bioni (2019), que critica a centralidade excessiva do consentimento como mecanismo de proteção, considerando-o insuficiente diante da complexidade das políticas de privacidade e da assimetria informacional entre usuários e empresas.

Para Bioni (2019), a proteção de dados exige mecanismos regulatórios robustos e o reconhecimento desse direito como autônomo em relação à privacidade clássica, especialmente diante da complexidade das políticas de privacidade e da assimetria informacional entre usuários e empresas.

No que tange à relação consumidor x fornecedor, o trabalho irá utilizar a tese da *assimetria informacional*, utilizando da obra de Laura Schertel Mendes como embasamento teórico, que defende a impossibilidade de mensuração exata das consequências do seu consentimento devida à assimetria de poder inerente das relações de consumo. Nas palavras de Mendes:

Por óbvio, não se trata de simplesmente “infantilizar” o titular dos dados, tratando-o como incapaz de decidir por si mesmo ou simplesmente ignorar sua capacidade racional. Porém, o foco excessivo na obtenção de seu consentimento (aparentemente) informado deixa de lado algo mais complexo: a real capacidade do titular dos dados pessoais de substancialmente compreender e avaliar os riscos e prejuízos que poderão advir de seu consentimento, sobretudo online (Mendes, 2014, p. 510-512).

Mendes defende ainda que o processamento impróprio de dados é por natureza difuso exigindo uma tutela jurídica coletiva, tratado como uma política pública autônoma, ponto este de extrema relevância para o trabalho que analisara a prática do profiling sob a perspectiva dos direitos difusos e coletivos, defendendo que a regulação deve ser pensada enquanto política pública e não apenas como um direito individual dos consumidores/ usuários.

Fechando os referenciais teóricos, para complementar discussões propostas agregaremos os estudos sobre colonialismo digital, desenvolvidas Faustino e Lippold (2023) e colonialismo de dados de Cassino, Souza e Silveira (2021). A escolha destes referenciais são uma forma de concentrar a discussão em um contexto brasileiro, utilizando como base teórica obras que foram elaboradas levando em consideração a complexidade brasileira incluindo as camadas sociais e raciais que certamente não podem ser ignoradas.

Sérgio Amadeu e Joyce Souza e João Francisco Cassino (2021), criticam a falta de regulação da transferência internacional de dados na LGPD (art. 33), e chamam a atenção

para o que denominaram no estudo de uma “não-questão” termo utilizado para questionar a ausência de debates sobre a acumulação de capital informacional de países periféricos, no qual se inclui o Brasil, e a relação dessa extração massiva de dados com o neocolonialismo, defendendo políticas de soberania digital através de investimentos em inteligência computacional local e soberania algorítmica e conhecimento tecnológico como um bem comum livre.

Deivison Faustino e Walter Lippold (2023) propõe uma discussão sobre a ligação entre a mente humana, e como os seres humanos estão sendo utilizados como meio para alimentar algoritmos, discutindo a lógica da mais valia nas relações digitais, sob a ótica dos pensadores Karl Marx e Frantz Fanon.

A abordagem teórica de Paul Ricoeur (1991) será incorporada à pesquisa para aprofundar a análise sobre os impactos do *profiling* sob a ótica da *teoria da identidade narrativa* desenvolvida pelo autor, que estuda a constituição do sujeito por meio da construção contínua de uma narrativa pessoal, integrando experiências passadas, presentes e expectativas futuras em uma história coerente de si mesmo, através da atribuição de sentido às próprias vivências de modo reflexivo e autônomo.

A partir desse referencial, será possível investigar de que maneira as práticas de *profiling*, ao coletar, analisar e direcionar informações pessoais, podem restringir ou condicionar a liberdade do sujeito de construir e reconstruir sua própria narrativa. Os algoritmos, ao influenciar o acesso a determinados conteúdos, sugerir comportamentos e moldar interações nas redes sociais, tendem a limitar as possibilidades de expressão e de autocompreensão, impactando diretamente o processo de desenvolvimento da personalidade. Assim, a teoria de Ricoeur oferece um arcabouço filosófico para compreender como a autonomia narrativa do indivíduo pode ser afetada pelas dinâmicas algorítmicas.

Tendo em vista que no contexto deste trabalho os dados são considerados um ativo fundamental da economia do conhecimento, utilizaremos dos ensinamentos do professor Paulo Bastos Tigre, sobre paradigmas tecnológicos para posicionar o modelo de negócio da empresa Meta na engrenagem da economia da informação ou, como nomenclatura utilizada pelo autor economia do conhecimento, aqui entendidas como sinônimos.

Diante do exposto, o referencial teórico apresentado oferece uma base sólida para compreender os múltiplos desafios e implicações do *profiling* em redes sociais, articulando questões de privacidade, assimetria informacional e capitalismo de vigilância e construção de identidade. Problematizando os impactos da perfilização no livre desenvolvimento da

personalidade. O trabalho evidencia a complexidade do tema e a importância a importância de políticas públicas que promovam o equilíbrio entre inovação tecnológica e salvaguarda dos direitos fundamentais.

2 A CONSTRUÇÃO JURÍDICA DAS LEIS DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL - DEFINIÇÃO E CLASSIFICAÇÃO

Nesta seção traremos a construção legislativa sobre privacidade e proteção de dados no Brasil. Serão analisados os conceitos de privacidade em suas diferentes abordagens doutrinárias, bem como a construção legislativa sobre o tema, partindo da Constituição brasileira e adentrando nas normas infraconstitucionais que surgiram ao longo dos anos de acordo com a necessidade de resposta à evolução social (Doneda, 2006. p. 33).

2.1 Privacidade e Proteção de Dados na Constituição Federal, previsão jurídica e evolução do instituto

Para fins deste trabalho, entende-se por privacidade o direito fundamental de controle sobre o fluxo de informações pessoais, abrangendo tanto a proteção contra intromissões indevidas quanto a capacidade de autodeterminação informativa. Esse conceito é dinâmico, contextual e deve ser compreendido à luz das transformações tecnológicas e sociais, especialmente no ambiente digital, onde a privacidade assume contornos relacionados à proteção contra usos abusivos e automatizados de dados pessoais.

A construção legislativa sobre privacidade e proteção de dados no Brasil parte de um diálogo entre conceitos históricos e demandas contemporâneas. A Constituição Federal de 1988 consagrou a inviolabilidade da vida privada como direito fundamental, o que em uma análise finalista poderia incluir os dados pessoais como um direito derivado da privacidade (Art. 5º, X). Porém, apenas com a Emenda Constitucional nº 115/2022 a proteção de dados pessoais foi elevada explicitamente a esse status, integrando o rol do Art. 5º e atribuindo à União competência exclusiva para legislar sobre o tema (BRASIL, 2022). Essa mudança refletiu a necessidade de adaptação do ordenamento jurídico a uma sociedade informatizada, onde dados pessoais passam a ser um ativo estratégico, especialmente no contexto econômico.

Em que pese a inclusão da proteção de dados no Brasil ter sido inserida por uma emenda constitucional apenas em 2022, faz sentido para a construção de raciocínio que este seja o primeiro dispositivo jurídico analisado, para que o leitor entenda a hierarquia normativa, visto que toda e qualquer norma infraconstitucional criada, ainda que anterior à Constituição, deve se adequar aos limites constitucionais estabelecidos.

Em 2022, a emenda constitucional nº 115 altera a Constituição Federal Brasileira para incluir o inciso LXXIX, do artigo 5º que insere a proteção de dados pessoais no rol de direitos e garantias fundamentais de terceira geração, também conhecidos como direitos difusos ou transindividuais, que surgem em resposta às demandas coletivas e globais, como o meio ambiente e a paz, necessários garantir a dignidade humana em um mundo digitalizado (Unaerp, 2024; Brasil, 2022).

Danilo Doneda explica os direitos fundamentais como sendo os instrumentos que protegem aspectos essenciais da personalidade humana, vinculados à dignidade e à autonomia do indivíduo, especialmente no contexto da sociedade contemporânea, não podendo ser reduzidos apenas a escolhas individuais, necessitando de mecanismos coletivos e normativos que assegurem proteção efetiva (Doneda, 2020).

O início dos debates sobre privacidade surge em 1890 com o artigo *The right to privacy*, de Warren e Brandeis (1890 *apud* Mendes, 2014, p. 583), que definem a privacidade como o “direito de ser deixado em paz”. Os autores denunciam como a fotografia, os jornais e outros aparatos tecnológicos permitiam o acesso e divulgação de fatos sobre a esfera privada da vida dos indivíduos de uma forma antes impensável.

Warren e Brandeis fundamentaram o direito à privacidade como proteção à inviolabilidade da personalidade, rompendo com a lógica anterior que associava a proteção da vida privada à propriedade do que é físico, passando a interpretar tal direito sob a ótica do princípio da inviolabilidade da personalidade, entendimento que influenciou a Constituição brasileira.

Da identificação do que é privacidade os autores definem uma série de hipóteses que a princípio não caracterizavam uma violação, entre eles o consentimento dos usuários sobre o que se deseja ou não tornar público. Nas palavras dos autores:

- (b) o direito à privacidade não veda a comunicação de tudo que é privado, pois se isso acontecer sob a guarda da lei, como, por exemplo, em um Tribunal ou em uma Assembleia Legislativa, não há violação desse direito;
- (c) a reparação não será exigível se a intromissão for gerada por uma revelação verbal que não cause danos; (d) o consentimento do afetado exclui a violação do direito; (Warren; Brandeis, 1890 *apud* Mendes, 2014, p. 491).

Celso Ribeiro de Bastos e Ives Gandra da Silva Martins (2001) destacam a dificuldade de se definir o alcance do conceito de privacidade diante das muitas possibilidades que variam

de acordo com o período e local, que modificam de forma substancial o contexto em que o termo está sendo analisado, nas palavras do autor:

Não é fácil demarcar com precisão o campo protegido pela constituição, É preciso notar que cada época dá lugar a um tipo específico de privacidade. Nos tempos atuais, seria tornar o dispositivo constitucional muito fraco ao considerar que ele abrangesse só o ocorrido nas casas dos particulares (Bastos; Martins, 2001, p. 71).

Irwin Altman conceitua a privacidade como uma vontade de gerenciamento e negociação contínua, um processo dinâmico, com limites a serem e refinados de acordo com a circunstância. No entendimento de Altman, o nível ótimo de privacidade é algo subjetivo alcançado quando se atinge o que é desejado pelo indivíduo, ou seja, o nível de contato com outros, a regulação de privacidade é então “*openness and closeness*”¹¹ (Altman, 1975)”.

Trazendo a discussão para as redes sociais, o contexto escolhido como objeto, as discussões sobre o significado de privacidade se intensificam, pois se torna extremamente mutável em função de diversos fatores como a localização do usuário, formas de uso, pessoas com quem deseja interagir, horário do dia entre outras variáveis.

Para Mikhail Vieira de Lorenzi Cancelier (2016), o conceito moderno de privacidade está profundamente ligado à proteção contra usos indevidos ou abusivos das informações pessoais, especialmente no ambiente digital, onde os registros podem ser armazenados e disseminados indefinidamente.

Daniel Solove (2008), em *Understanding Privacy* (2008), argumenta que a privacidade é um conceito plural, composto por diferentes dimensões e interesses, incluindo proteção contra invasão, divulgação indesejada, uso indevido e distorção de informações pessoais. Solove propõe uma “teoria pragmática da privacidade”, na qual o foco está nas práticas e nos danos concretos que violam a privacidade, em vez de buscar uma definição universal e abstrata.

Sobre a relação entre privacidade e contexto, Ariel Soares Teles, em sua tese de doutorado, realizou uma pesquisa com 164 brasileiros para testar a ferramenta *SelPri*, integrada ao Facebook, que permite aos usuários adaptarem as configurações de privacidade de suas postagens conforme diferentes situações, como trabalho, casa ou estudo. Os resultados indicaram que a maioria dos usuários gostariam de proteger suas informações de forma mais

¹¹ Controle da “abertura” ou “fechamento”, imposição de limites, para acesso a algo que é considerado privado pelo indivíduo, por exemplo, informações pessoais.

eficaz no ambiente online, com 80% dos participantes considerando a solução útil para garantir a privacidade (Teles, 2017).

Todavia, trazendo a discussão para o contexto da presente pesquisa, observa-se que a vontade dos usuários em ajustar a privacidade não seria possível, pois a solução apresentada por Ariel se aplica apenas às postagens dos usuários e não ao acesso que a plataforma tem aos dados, já que nos aplicativos Instagram e Facebook o consentimento for dado pelo usuário uma única vez, não havendo uma ferramenta da própria plataforma em que o usuário possa acessar e/ou modificar quaisquer das licenças concedidas, ou mesmo solicitar a retirada de alguma informação pessoal que entender violar a sua privacidade.

Em síntese, as principais teses sobre privacidade incluem: (i) o direito de ser deixado em paz (Warren e Brandeis), (ii) a privacidade como controle sobre informações pessoais (Westin, Solove), (iii) a privacidade como processo dinâmico de negociação (Altman), (iv) a privacidade contextual (Nissenbaum), e (v) a proteção contra usos indevidos de dados pessoais, especialmente no ambiente digital (Cancelier). Essas perspectivas evidenciam a complexidade e a multidimensionalidade do conceito de privacidade, exigindo uma abordagem integrada e atualizada no ordenamento jurídico brasileiro.

Atualmente a Constituição prevê de forma expressa que a proteção ao instituto inclui os meios digitais, e consequentemente as redes sociais¹² atribuindo a responsabilidade de fiscalização, proteção e tratamento dos dados à União (Brasil 1988). Todavia, quanto à eficácia, é classificada como norma de eficácia limitada, aquela cuja concretização depende de regulamentação infraconstitucional complementar ao texto definindo a forma como tal direito será efetivado em cada contexto (Silva, 2019).

Em síntese, a evolução do instituto da privacidade e da proteção de dados no Brasil reflete a necessidade de adaptação do ordenamento jurídico às novas realidades tecnológicas e sociais. O conceito de privacidade, inicialmente associado à inviolabilidade da personalidade, ampliou-se para abranger à autodeterminação informativa e a proteção contextual dos dados pessoais, especialmente no ambiente digital.

No entanto, a efetividade desses direitos depende da complementação por normas infraconstitucionais, que detalham os mecanismos de proteção e os deveres dos agentes de tratamento. Dessa forma, a análise da legislação infraconstitucional, como o Código de

¹²Art. 5º LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Defesa do Consumidor e o Marco Civil da Internet, torna-se fundamental para compreender a efetividade da proteção de dados no país, tema que será desenvolvido nos itens subsequentes.

2.2 Código de Defesa do Consumidor (CDC)

Iniciando o estudo das setoriais, analisaremos as contribuições da lei 8.078/90 também conhecida como Código de Defesa do Consumidor (CDC, 1990) sobre privacidade e proteção de dados. A linha interpretativa adotada parte de uma leitura finalista, orientada pela função social da norma e pela realidade das relações de consumo mediadas por tecnologias digitais, posicionamento que tem sido adotado pela doutrina e jurisprudência brasileira, conforme veremos ao longo do desenvolvimento do texto.

O Código de Defesa do Consumidor assume especial relevância na proteção dos usuários de redes sociais diante das práticas de perfilização e tratamento massivo de dados pessoais. Ao reconhecer a vulnerabilidade do consumidor e impor deveres de transparência e boa-fé aos fornecedores, o CDC oferece uma base normativa robusta para equilibrar relações marcadas por forte assimetria informacional, incluindo o ambiente digital. Essa perspectiva é fundamental para o presente item, que busca compreender como a legislação consumerista pode mitigar os riscos à autodeterminação informativa e ao livre desenvolvimento da personalidade nas plataformas da Meta.

Embora não tenha sido pensado especificamente para o tema privacidade, proteção de dados e redes sociais, o Código de defesa do consumidor foi a primeira lei a tratar o tema de forma moderna, visando as novas tecnologias de processamento de dados, servindo como embasamento para importantes decisões que reconheceram a natureza jurídica da relação entre redes sociais e usuários, qual seja, uma relação de consumo (Brasil, 1990; Mendes, 2014).

Classificado como norma de ordem pública e de interesse social, o CDC encontra fundamento na própria Constituição Federal, no artigo 170, inciso V, que estabelece a defesa do consumidor como princípio da ordem econômica devendo se aplicar a pessoas físicas, jurídicas e às coletividades, promovendo proteção ampla nas relações de consumo (Castro, 2023, p. 11; Brasil, 1990)¹³.

¹³CDC, Art. 1º O presente código estabelece normas de proteção e defesa do consumidor, de ordem pública e interesse social, nos termos dos arts. 5º, inciso XXXII, 170, inciso V, da Constituição Federal e art. 48 de suas Disposições Transitórias.

O Código de Defesa do Consumidor (CDC) foi criado para equilibrar as relações entre consumidores e fornecedores, sob o argumento de trazer igualdade material, implementando mecanismos de proteção à parte mais vulnerável da relação contratual. Seu objetivo é restabelecer o equilíbrio, aplicando-se a todas as situações em que estejam presentes, um fornecedor e um consumidor, assim definidos nos artigos 2º e 3º, incluindo a coletividade de pessoas, ainda que indetermináveis, vejamos:

Art. 2º Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final.

Parágrafo único. Equipara-se a consumidor **a coletividade de pessoas, ainda que indetermináveis**, que haja intervindo nas relações de consumo.

Art. 3º: Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços. (Brasil, 1990, grifo nosso).

Em um primeiro momento, a aplicação do Código de Defesa do Consumidor (CDC) aos serviços prestados por plataformas de redes sociais suscitou, controvérsias na doutrina, sobretudo em razão da ausência de pagamento direto pelos usuários. A prestação gratuita do serviço levou parte da doutrina a questionar se estariam configurados os elementos essenciais à caracterização de uma relação de consumo.

Entretanto, esse entendimento foi progressivamente superado tanto pela doutrina quanto pela jurisprudência nacional, sendo pacificado pelo Poder Judiciário brasileiro prevalecendo o entendimento de que a gratuidade aparente não afasta, por si só, a incidência do CDC. A fundamentação para tal conclusão reside no fato de que a remuneração pode se dar de forma indireta, por meio da coleta e exploração econômica de dados pessoais, publicidade dirigida e outros mecanismos típicos da economia digital.

Para Doneda (2021), a gratuidade nas plataformas digitais mascara um modelo de monetização baseado na coleta e uso de dados pessoais, o que reforça a existência de uma contraprestação e, portanto, de uma relação jurídica de consumo.

No mesmo sentido, o Superior Tribunal de Justiça, reconheceu que a ausência de pagamento direto, por si só, não é motivo justo para afastar a incidência do CDC nas relações entre usuários e plataformas digitais, uma vez que a remuneração pode ocorrer de forma indireta por meio da exploração econômica dos dados pessoais (Brasil, STJ, REsp 1.316.921/RJ, 2012).

Compreendeu-se que a ausência de contraprestação financeira não compromete a presença dos elementos estruturantes da relação de consumo. Ao contrário, revela-se a existência de vínculo contratual atípico, mas juridicamente relevante, no qual o provedor do serviço de rede social assume papel inequívoco de fornecedor, conforme definição da própria lei, sendo inaplicável qualquer tentativa de dissociação entre a figura do provedor de serviços digitais e os parâmetros normativos próprios das relações de consumo.

A jurisprudência sobre o tema foi proferida no Recurso Especial 1.316.921 RJ 2011/0307909-6, no caso envolvendo a apresentadora Maria da Graça Xuxa Meneghel e a Google Brasil Internet LTDA e teve como relatora a ministra do Superior Tribunal de Justiça Nancy Andrigh que abordou a questão em seu relatório:

Na lição de Cláudia Lima Marques, a expressão "remuneração" permite incluir todos aqueles contratos em que for possível identificar, no sinalagma escondido (contraprestação escondida), uma remuneração indireta do serviço (**Comentários ao código de defesa do consumidor: arts. 1º ao 74**. São Paulo: RT, 2003, p. 94). No caso da GOOGLE, é clara a existência do chamado cross marketing – ação promocional entre produtos ou serviços em que um deles, embora não rentável em si, proporciona ganhos decorrentes da venda de outros. Apesar das pesquisas realizadas via GOOGLE SEARCH serem gratuitas, a empresa vende espaços publicitários no site, bem como preferências na ordem de listagem dos resultados das buscas. (Brasil, STJ/2011, grifo do autor).

Aqui vale abrir um breve parêntese para destacar a importância de empresa google na economia informacional, pois foi a empresa que inaugurou o modelo de negócio que utiliza os dados como principal ativo, e inclusive se mantém ainda hoje entre as principais *big techs* que monopolizam a economia de dados, integrando o chamado GAFAM, que será objeto de estudo em item próprio.

Reconhecer a relação de consumo é de extrema relevância, pois significa admitir a vulnerabilidade do consumidor, havendo um desequilíbrio preexistente entre as partes, o que permite uma exceção à regra da não intervenção do estado nas relações privadas, pois leva-se em conta a limitação técnica de compreensão do consumidor, possibilitando uma relação igualitária (Mendes, 2014).

Sobre a relação de desequilíbrio o CDC trabalha com duas hipóteses, a primeira é de caráter material, que considera a vulnerabilidade do consumidor, característica intrínseca de toda a relação de consumo, conforme art. 4º, inciso I, do instituto. A segunda é de ordem

processual, que está ligada a situação concreta em que o consumidor se encontra em determinado processo, prevista no artigo 6º, inciso VIII do instituto (Brasil, 1990).

Em que pese a semelhança entre os conceitos, é importante trazer esta diferenciação para que tais institutos não se confundam, pois enquanto a vulnerabilidade é presumida e alcança todos os consumidores, a hipossuficiência é um instituto de natureza técnica, não presumida, que surge quando além de ser a parte mais vulnerável o consumidor também tem uma impossibilidade técnica de produzir as provas de seu direito.

Neste trabalho compartilhamos do posicionamento que em um ambiente de rede social o usuário é ao mesmo tempo vulnerável por não ter a possibilidade de estar em condição de igualdade na relação com a empresa e hipossuficiente, devido à dificuldade de comprovar eventual direito subjetivo violado por uma rede social, necessitado da intervenção do estado para estabelecer o equilíbrio.

Com mencionado no item anterior, a Constituição disciplina os comandos gerais, cabendo à legislação infraconstitucional dizer o como tal direito será organizado em cada matéria. As normas especiais são criadas quando se identifica a necessidade de proteção ou regulamentação mais detalhada para determinados grupos, relações jurídicas ou contextos sociais, visando atender de maneira adequada as particularidades que as normas gerais não conseguem alcançar (Castro, 2023).

Classificado como norma de ordem pública e de interesse social, o CDC encontra fundamento na própria Constituição Federal, no artigo 170, inciso V, que estabelece a defesa do consumidor como princípio da ordem econômica devendo se aplicar a pessoas físicas, jurídicas e às coletividades, promovendo proteção ampla nas relações de consumo (Castro, 2023; Brasil, 1990).

De acordo com Cláudia Lima Marques (1994), o CDC exerce tríplice função, qual seja: promover a defesa do consumidor; assegurar o princípio geral da atividade econômica necessária à defesa do consumidor, art. 170, V, da CRFB; e ordenar a tutela especial infraconstitucional, art. 48, do ato das Disposições Constitucionais Transitórias da Constituição Federal de 1988 (Revista de Direito Internacional Econômico e Tributário, p.18, citado por Castro, 2023).

Estabelecidos os atores aos quais a lei se aplica, o diploma avança para o artigo 4º, princípios da relação de consumo, que estabelece uma série de objetivos, para consumidores, fornecedores e ao estado brasileiro, como a necessidade de proteção efetiva e equilíbrio de interesses entre proteção do consumidor e desenvolvimento tecnológico. (CDC 1990).

Trazendo os princípios para a pesquisa, pode-se constatar que o legislador, apesar de reconhecer a vulnerabilidade do consumidor, não estabelece uma hierarquia sobre quais direitos devem prevalecer, mas propõe um equilíbrio de interesses, de maneira que não haja uma dicotomia entre tecnologia e privacidade (Mendes, 2014, p. 577). Entretanto, como pontuado por Naína Ariana Souza Tumelero (2021), se analisado o objetivo do CDC, ainda que indique outros direitos concomitantes, resta claro que o consumidor é o sujeito núcleo da proteção do instituto.

Apesar de sua função social e do caráter protetivo em relação ao consumidor, o Código de Defesa do Consumidor (CDC) deve ser interpretado em harmonia com outros princípios constitucionais, como o direito à livre iniciativa e o interesse econômico. Dessa forma, a proteção conferida ao consumidor não é absoluta, devendo ser ponderada à luz do caso concreto e em conjunto com outros direitos fundamentais.

Nessa perspectiva, o CDC atua como base interpretativa, sendo aplicado de forma subsidiária quando não houver norma específica, prevalecendo esta última em situações de conflito aparente de normas, conforme o princípio da especialidade. A análise comparativa entre o CDC e a Lei Geral de Proteção de Dados (LGPD) revela a necessidade de uma abordagem integrada para a efetiva proteção dos direitos do consumidor, especialmente diante dos desafios impostos pelo tratamento de dados pessoais nas relações de consumo digitais.

Enquanto o CDC se preocupa de cuidar de toda a cadeia de consumo, a LGPD, originalmente estruturada para regular o tratamento de dados pessoais em geral, não detalha de forma específica e exaustiva as particularidades e desafios de todas as etapas e agentes envolvidos na cadeia complexa de tratamento de dados em um contexto de consumo. Ao mesmo tempo que a LGPD reconhece a vulnerabilidade do consumidor, concede a este o direito de consentimento para o tratamento de seus dados quase que de maneira irrestrita o que pode configurar uma contradição entre os institutos.

Ponto relevante é que nenhum dos institutos faz menção expressa ao *profiling*, diferente da *General Data Protection Regulation* (GDPR), legislação europeia que inspirou a LGPD. Que optou por tratar o tema de forma específica em seu artigo 4º:

Definição de perfis: qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspectos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspectos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações (GDPR DIGEST, 2025).

No contexto brasileiro é possível que a depender do caso concreto o tema careça de uma solução legislativa mais eficaz, necessitando nesta hipótese, da combinação entre institutos, para solucionar os problemas de acordo com o caso concreto, e nesta combinação o CDC seria considerado como base interpretativa e reafirmação da vulnerabilidade e assimetria informacional dos usuários.

Avançando na análise do CDC temos o princípio da Transparência e informação clara, previsto nos arts. 4º, 6º, III, e 31 da lei, que determina que a informação entregue ao usuário seja apresentada de maneira adequada e clara quanto aos produtos ou serviços que serão oferecidos. Todavia, da leitura dos termos de uso percebe-se uma imprecisão sobre como é feita a perfilização do usuário, vejamos: “Ao usar nossos produtos, você concorda que podemos mostrar anúncios que consideramos como possivelmente relevantes para você e seus interesses. Usamos seus dados pessoais para ajudar a determinar quais anúncios personalizados serão mostrados a você” (Facebook, 2025).

Para que a informação seja considerada transparente, é fundamental que o titular dos dados compreenda o que será feito com suas informações e de que forma isso ocorrerá; caso contrário, não será possível ao consumidor ter plena ciência sobre o destino de seus dados, ou a forma como tal procedimento pode o impactar, conforme dispõe o art. 6º, VI, do CDC.

A dificuldade do usuário está em entender qual o caminho de seus dados no período pós consentimento, pois ainda que a plataforma informe quais dados serão coletados, a coleta é apenas parte da cadeia de tratamento sucedida pelo processamento, armazenamento, critérios técnicos de automatização, e esta falta de precisão causa opacidade, inviabilizando a transparência para com os usuários.

Neste sentido, Bioni (2019, p. 127) ressalta que o CDC, art. 43,¹⁴ cuida dos direitos do consumidor de forma ampla em relação aos bancos de dados, dando abrangência ao artigo para que alcance todo e qualquer dado pessoal, para que não se limite a pensar o banco de dados apenas como parâmetros de avaliação de crédito, nas palavras do autor: “A racional do legislador foi alcançar todo e qualquer banco de dados que atinja o livre desenvolvimento da personalidade do consumidor”.

Entretanto, o CDC não é claro sobre qual os regramentos para a manipulação de dados não pessoais ou informações obtidas por inferência. O que dificulta ao consumidor a real

¹⁴Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

compreensão de como seus dados são tratados, consequentemente afetando a transparência da relação prevista no art. 6º, III, e 31.

A transparência e informação clara, exigem que o fornecedor entregue a informação ao usuário de maneira compreensível, sobre os produtos ou serviços que serão oferecidos, entretanto os termos de uso das plataformas por muitas vezes apresentam textos extensos e linguagem técnica, de forma que não fica claro sobre como se dá a coleta e tratamento dos dados, dificultando a finalidade da Lei já que a ausência de transparência impede um consentimento informado e eficaz do ponto de vista material.

Sobre a falta de transparência, pesquisa realizada pelo NetLab, laboratório vinculado à Escola de Comunicação da Universidade Federal do Rio de Janeiro (UFRJ), constatou que nenhuma das principais empresas de rede social atingem a pontuação considerada ideal em grau de transparência e de qualidade de dados. Entre as *big techs* analisadas está o Instagram, que em uma escala de 0 a 100 alcançou apenas 52,1 pontos, sendo classificado como regular. o que demonstra uma deficiência da plataforma em cumprir de forma satisfatória o requisito da transparência e consequentemente de se adequar ao CDC (Gama, 2024).

O Facebook explica em seus termos de uso sobre a experiência personalizada que é feita a partir dos dados dos usuários. Entretanto, da leitura do texto não é possível aferir quais são os limites da captação de dados feita pela plataforma e quais os destinos desses dados. A plataforma informa apenas que serão utilizados “dentro e fora” dos produtos da empresa” o que gera dúvida razoável quanto à finalidade do uso. Vejamos:

Sua experiência no Facebook não se compara à de mais ninguém: desde as publicações, os stories, os eventos, os anúncios e outros conteúdos que você vê no Feed do Facebook ou na nossa plataforma de vídeo até as Páginas do Facebook que você segue e outros recursos que pode usar, como o Facebook Marketplace e a pesquisa. Por exemplo, usamos os dados sobre as conexões que você faz, as escolhas e as configurações que seleciona e **o que compartilha e faz dentro e fora dos nossos Produtos** para personalizar a sua experiência. (Meta, 2025, grifo nosso).

Importante ressaltar que a presente pesquisa não se destina a discutir um dano em tese, mas de trazer luz a uma série de casos envolvendo a empresa ao longo dos anos, formando dúvida razoável de que os dados dos usuários são utilizados para finalidades diversas, que extrapolam a finalidade informado pelos termos de uso, qual seja a perfilização para fins de melhoria na experiência e oferecimento de anúncios. Para fins de fundamentar esta informação, alguns desses casos serão abordados ao longo da pesquisa.

Sobre forma de tratamento dos dados, a pesquisa não logrou êxito em encontrar, em meios oficiais da plataforma, como é feita a formação de perfil e/ou quais conteúdos serão expostos, demonstrando uma opacidade no modo de operação dos aplicativos da empresa.

Fato é que ao tempo da edição de uma lei não é possível prever todas as evoluções sociais, de maneira que se faz constantemente necessário a atualização das leis, bem como a edição de novas normas mais específicas que se adequem ao momento atual.

Sugere-se então uma atualização do MCI, para incluir normas específicas sobre transparência algorítmica, direito à explicação das decisões automatizadas e mecanismos de controle do usuário sobre seu perfil digital. Um avanço possível seria a previsão de relatórios de impacto à privacidade para operações de *profiling*, inspirado no art. 38 da LGPD, e a exigência de que as plataformas ofereçam ferramentas para que o usuário acesse, corrija ou conteste o perfil construído sobre si, garantindo assim maior efetividade à autodeterminação informativa e ao livre desenvolvimento da personalidade (Brasil, 2018; ANPD, 2023).

Todavia, ainda que não pensado especificamente no contexto de redes sociais e proteção de dados o CDC, é capaz de promover algum grau de proteção aos usuários em relação às práticas de perfilização, em especial se analisada de maneira finalista e em conjunto com outras legislações, sendo comumente utilizado com fundamentação em decisões judiciais envolvendo os usuários e as redes sociais da empresa Meta.

Neste item a pesquisa tentou demonstrar a prática de *profiling* à luz da relação de consumo, observou que o instituto não menciona expressamente a prática, mas é capaz de trazer subsídios mínimos de proteção aos consumidores/usuários, sendo utilizado subsidiariamente pelo judiciário brasileiro para fundamentar decisões sobre a responsabilidade dos provedores de serviço e plataformas digitais.

2.3 O Marco Civil da Internet, edição e abrangência

Em resposta aos desafios do mundo digital que crescem aceleradamente, o Brasil vem buscando criar uma estrutura legal sólida para proteger a privacidade e os dados pessoais no ambiente digital. Neste contexto é editada a Lei 12.965/2014, também conhecida como Marco Civil da Internet (MCI), que estabelece princípios, garantias, direitos e deveres para o uso da Internet no país (Brasil, 2014).

O Marco Civil da Internet assume papel importante na proteção dos usuários de redes sociais, ao estabelecer princípios como neutralidade, privacidade e autodeterminação

informativa, necessários para a tutela dos direitos fundamentais no ambiente digital, além de trazer os comandos de boas práticas no ambiente digital, no qual se inclui a proteção dos dados pessoais, tida como um de seus pilares, ao lado da neutralidade de rede e da liberdade de expressão (Arruda, 2021; Bioni, 2019).

Para fins do MCI as redes sociais são consideradas provedores de aplicação de internet, assim definidas pelo artigo 5º, VII, como:

Qualquer pessoa natural ou jurídica que oferece um conjunto de funcionalidades acessíveis por meio de um terminal conectado à internet, devendo se submeter à legislação brasileira quando realizarem operações de: coleta, armazenamento, guarda e tratamento de registros de dados pessoais, classificação na qual se enquadra o serviço de rede social ou de comunicações em território nacional (Brasil, 2014; Brasil, STJ, 2022).

Quanto aos usuários, ocupam a figura de titulares, entendido como as pessoas naturais usuárias da plataforma¹⁵. No contexto da Lei Geral de Proteção de Dados Pessoais (LGPD), a Meta Platforms Inc. atua como agente de tratamento, sendo responsável pelas operações de tratamento de dados realizadas nos aplicativos Instagram e Facebook, conforme os incisos V e XI do artigo 5º da LGPD. Simultaneamente, a empresa também é classificada como provedora de aplicação de internet, nos termos do Marco Civil da Internet (MCI), sujeitando-se, portanto, a ambos os regimes normativos (Brasil, 2018; Brasil, 2014; ANPD, 2024).

Em síntese, o Marco Civil da Internet fornece subsídios importantes para a proteção do usuário ao reconhecer a autodeterminação informativa e exigir transparência e controle sobre o tratamento de dados pessoais sendo utilizado para embasar decisões judiciais e administrativas para exigir maior clareza e responsabilidade das plataformas digitais, especialmente em casos envolvendo práticas abusivas de coleta e uso de dados. Contudo não há uma regra estabelecida para como deve ser o consentimento nestes casos, ou qual a lei deveria cuidar desta problemática, se o MCI ou a LGPD.

O MCI pode ser utilizado para mitigar os riscos à autonomia e à autodeterminação informativa dos usuários, especialmente em contextos de coleta massiva e tratamento automatizado de dados. No entanto, a efetividade do consentimento como ferramenta de controle ainda é limitada diante da complexidade técnica, da assimetria informacional, e das

¹⁵O trabalho utilizará a nomenclatura de acordo com a redação da legislação que está sendo analisada, MCI, entretanto, eventualmente utilizaremos o termo consumidores, entendidos na pesquisa como sinônimos.

lacunas jurídicas, reforçando a necessidade de uma abordagem integrada entre MCI, LGPD e CDC (Bioni, 2019; Doneda, 2021).

O Marco Civil, assim como na LGPD utiliza o consentimento do usuário como principal base legal para tratamento de dados pessoais, todavia as legislações trataram do tema de forma parcialmente diferente. Importante mencionar que o Marco Civil foi editado em 2014, quatro anos antes da Lei Geral de Proteção de Dados, de modo que não poderia ao tempo de sua edição mencionar a lei ou mesmo se adequar a ela. (Brasil. 2014).

A ordem cronológica da edição das leis traz implicações quanto à aplicabilidade de determinados dispositivos, que podem ser expressas ou tacitamente revogados pela lei posteriormente editada, \aa exemplo do art. 7º, Incisos VII e IX do MCI (Bioni, 2019)

No art. 7º, Incisos VII e IX¹⁶ do Marco Civil da Internet, os requisitos do consentimento para o tratamento de dados por terceiros precisava ser: livre, **expresso** e inequívoco, baseado na proposta de que o titular deveria seguir seus dados em todos os seus movimentos, ou seja, maior carga de participação do titular de dados. (Bioni, 2019, grifo nosso).

Todavia, a LGPD não reproduziu o texto na íntegra, trazendo em sua redação que o consentimento deve ser, uma manifestação livre **informada** e inequívoca, art. 5º, XII, mantendo o consentimento de forma expressa apenas aos dados pessoais sensíveis, art. 11. 1 LGPD (Bioni, 2019, grifo nosso).

O consentimento informado requer que o ato de consentir seja consciente, de forma que não deixe dúvida sobre a intenção do usuário em autorizar o tratamento de seus dados, não necessitando que seja necessariamente escrito ou destacado das demais cláusulas. Já o consentimento expresso exigiria maior carga participativa do titular, incluindo por exemplo cláusulas mais descriptivas e destacadas das demais, o que na prática torna a LGPD menos rigorosa quanto ao consentimento (Arruda, 2021, p. 90; Bioni, 2019, p. 203).

Bioni critica a adoção do termo “específico” por acreditar ser redundante, argumentando que em um cenário de proteção de dados qualquer consentimento deveria ser necessariamente direcionado para um propósito específico e explícito, de acordo com o princípio da finalidade, sendo intrínseco a uma declaração de vontade. O autor argumenta que

¹⁶ Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; IX - Consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

do ponto de vista técnico seria melhor que a LGPD tivesse mantido a mesma redação do MCI, entendendo que semanticamente o termo “expresso” representaria um nível de interação mais intenso (Bioni, 2019, p. 202-203).

Por ter sido editada especificamente para regular o tratamento de dados pessoais, inclusive nos meios digitais, a redação da LGPD substitui a do MCI na hipótese de um conflito aparente de normas, por ser norma posterior e mais específica sobre dados, em obediência ao princípio da especialidade, sendo assim, aplicar-se-á o termo *informado* (LGPD), em vez de *expresso* (MCI), gerando a derrogação tácita do artigo 7º, incisos VII e IX, do Marco Civil da Internet, como explica Maximiliano:

quando cessa em parte a autoridade da lei, ou do costume, dá-se a derrogação; quando se extingue totalmente, é o caso de ab-rogação. Um termo genérico - revogação abrange um e outra hipótese. [...] A revogação é expressa, quando declara a lei nova; tácita, quando resulta, implicitamente, da incompatibilidade entre o texto anterior e o posterior (Maximiliano, 2006, p. 291-292).

Em que pese discussões doutrinárias sobre o tema, prevalece o entendimento pela revogação parcial da norma, na modalidade tácita, com fundamentos no princípio da especialidade e no artigo 2º da Lei de Introdução às Normas de Direito Brasileiro¹⁷, a exigência de procedimento mais rigoroso (expresso) permanece apenas quanto aos dados sensíveis, ou àqueles que possam revelar dados pessoais sensíveis¹⁸, nos quais se mantém a necessidade de maior carga participativa do usuário (LGPD, 2018; Maximiliano, 2006).

2.4 O consentimento como base legal para *profiling*

Como proposto nos objetivos específicos da pesquisa, neste item analisaremos o consentimento como base legal apropriada para a prática de *profiling* especificamente no ambiente das redes, analisando a forma e os efeitos do instituto que tem sido fortemente questionado pela doutrina brasileira, no qual este trabalho fará suas contribuições.

¹⁷ Art. 2º Não se destinando à vigência temporária, a lei terá vigor até que outra a modifique ou revogue. § 1º A lei posterior revoga a anterior quando expressamente o declare, quando seja com ela incompatível ou quando regule inteiramente a matéria de que tratava a lei anterior.

¹⁸ Art. 5º Para os fins desta Lei, considera-se: II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

Para Doneda (2021), o modelo atual de consentimento nas redes sociais é insuficiente para garantir que o usuário comprehenda efetivamente o destino e o tratamento de seus dados, especialmente diante da opacidade dos algoritmos e da assimetria técnica e informacional entre as partes. O autor pontua que a mera disponibilização de informações não é suficiente para assegurar o controle do usuário sobre seus dados, de modo a fortalecer a proteção dos direitos fundamentais do consumidor (Doneda, 2021; Bioni, 2019).

Bioni (2019) reconhece a importância do MCI como um reforço a proteção da privacidade e a autodeterminação informativa como princípio estruturante da relação entre usuário e provedor, mas assim como Doneda (2021) critica o uso do consentimento como base legal única, sob o argumento de que a complexidade e o volume de dados nas plataformas tornam inviável uma decisão genuína e informada por parte dos usuários (Bioni, 2019).

Como possíveis soluções, Bioni levanta a possibilidade de procedimentos que chamem a atenção do autor para o ato, como por exemplo, mensagens textuais explicativas, imagens, combinação de ambos, ou uma dupla verificação a partir da combinação de canais, como por exemplo, autorização por e-mail e posteriormente por mensagem de texto Bioni (2019). Em que pese o autor pontuar sobre a pressão social de estar nas redes sociais, as discussões circulam majoritariamente entre a relação entre consentimento x autodeterminação informativa.

Contudo, as críticas dos autores se concentram na hipossuficiência técnica dos usuários, conectando-se com o princípio da autodeterminação informativa, de modo que o problema do consentimento poderia ser solucionado aumentando o nível de consciência do usuário sobre a utilização de seus dados.

Ocorre que ao submeter esses estudos sobre consentimento nas redes sociais da empresa Meta adicionam-se algumas particularidades à relação entre usuários e plataforma, das quais não passam apenas por questões de maior domínio dos usuários sobre seus dados, mas também sobre o papel que as redes sociais exercem na rotina dos cidadãos brasileiros, que como já exposto, ocupam o terceiro lugar na lista de países que mais consomem a internet no Brasil.

Além de exercerem papel relevante na vida social, plataformas como Instagram e Facebook estruturam seu modelo de negócio na modalidade conhecida como *take it or leave it*. Esse termo, traduzido como “aceite tudo ou nada”, significa que o usuário não tem a possibilidade de negociar ou ajustar os termos de uso: para acessar os serviços, é preciso

aceitar integralmente as condições impostas pela empresa. Nessa lógica, embora o acesso às redes sociais seja aparentemente gratuito, o usuário realiza um pagamento indireto ao ceder seus dados pessoais, que passam a ser utilizados como principal recurso econômico da plataforma. Não há, portanto, alternativa de acesso sem a concordância com essa troca, tornando o fornecimento de dados uma condição obrigatória para o uso dos serviços.

Importante mencionar que o consentimento na modalidade *take it or leave it*, nas redes sociais apresentado pelo termo “li e concordo”, não apenas permite o acesso aos dados dos usuários, mas também impõe uma série de cláusulas de natureza contratual por adesão, aquela sem qualquer margem de negociação entre consumidor e fornecedor, que não é vedado legalmente por nenhum instituto, sendo portanto permitido nos termos do art. 122 do Código Civil¹⁹ formando uma lacuna jurídica explorada por plataformas como Facebook e Instagram.

Por este motivo entendemos que a redução da opacidade resolveria parcialmente o problema do consentimento, pois ainda que seja destacado e o nível de consciência técnico do usuário fosse elevado a um ponto que o permitisse entender efetivamente sobre o que está autorizando, ainda assim o consentimento poderia estar viciado, pois a redução da opacidade seria uma solução parcial da autodeterminação informativa.

Considerando que entre os requisitos do consentimento está a liberdade, ou seja, precisa ser *livre*, além de informado e inequívoco, o aumento de consciência e carga participativa do usuário supriria o requisito da informação, entretanto o que questionamos neste item é sobre o requisito da liberdade, tecendo a crítica que, diante de uma escolha binária em que o não aceitar implicaria em um custo social, a escolha não pode ser efetivamente livre.

Por este motivo, permaneceriam as implicações quanto ao livre desenvolvimento da personalidade, já que este guarda relação com a autonomia da pessoa para se desenvolver conforme suas escolhas e valores, livre de interferências indevidas, direito este que entendemos não ser pleno diante de uma relação contratual, em que a não aceitação implicaria automaticamente na exclusão e no não pertencimento a um ambiente social.

Trazendo as considerações do Código Civil brasileiro sobre os vícios de consentimento em matéria de contratos, a validade do consentimento em uma relação contratual pode estar viciada nas seguintes hipóteses:

¹⁹ Art. 122. São lícitas, em geral, todas as condições não contrárias à lei, à ordem pública ou aos bons costumes; entre as condições defensas se incluem as que privarem de todo efeito o negócio jurídico, ou o sujeitarem ao puro arbítrio de uma das partes

- i) Erro (arts. 138-144): caracterizado pela falsa percepção da realidade que leva uma das partes a celebrar o contrato, podendo se subdividir em erro substancial, aquele relativo à natureza ou ao objeto do contrato, ou erro accidental, quando relativo a circunstâncias que não afetam o contrato.
- ii) Dolo (arts. 145-150), caracterizado pela manobra enganosa por uma das partes para induzir a outra a celebrar o contrato, e se subdivide em positivo, ação de enganar, ou negativo, omissão de informações relevantes.
- iii) Coação (arts. 151-155), pressão física ou psicológica exercida sobre uma das partes para que esta celebre o contrato.
- iv) Estado de perigo (art. 156), Exploração de situação de necessidade premente que leva a parte a aceitar condições manifestamente desvantajosas;
- v) Lesão (art. 157).

A pesquisa compactua com a ideias de que o consentimento nas redes sociais Facebook e Instagram, precisa ser analisado sob ao menos três perspectivas:

A primeira referente à opacidade do tratamento, causada pela falta de informações específicas sobre o caminho percorrido pelos dados, bem como o real uso destes dados por parte de seus agentes controladores, caracterizando um vício de dolo, de modo negativo, pela omissão de informações relevantes.

A segunda camada guarda relação com a pressão social, a necessidade de estar naquele ambiente e guarda mais relação como o instituto da coação, na modalidade psicológica e estrutural, que motiva o usuário de estar ali pelas oportunidades sociais que os aplicativos têm a oferecer.

A terceira diz respeito a lesão, art. 157. Art. *Ocorre a lesão quando uma pessoa, sob premente necessidade, ou por inexperiência, se obriga a prestação manifestamente desproporcional ao valor da prestação oposta.* Aqui se questiona a proporcionalidade, aquilo que se recebe em troca do que é dado. Aqui compactuamos com a ideia de que devido a coação estrutural o usuário tende a consentir como os termos de uso da plataforma não apenas por querer utilizar o serviço, mas também pela pressão de pertencer a este meio social, o que impossibilita a este a análise de uma balança justa entre o que se recebe em troca do que se oferece, incidindo assim no vício de lesão devido a uma sinalagma desproporcional.

Vale ressaltar que os vícios de consentimento tratados pelo código civil, acima mencionados, foram pensados para contratos civis tradicionais, dos quais a pesquisa se propôs

a fazer uma analogia ao traçar um paralelo entre os vícios de consentimento tradicionais e o consentimento para tratamento de dados para fins de *profiling*.

Desta forma, a vulnerabilidade não pode ser sanada apenas por atitudes individuais dos usuários, mas sim por uma intervenção do estado para reestabelecer o equilíbrio entre as partes, atuando como agente garantido da ordem social.

Para fundamentar a intervenção do Estado no modelo de consentimento estudado, utilizaremos da teoria do fato social de Émile Durkheim, por entendermos as plataformas como mecanismos coletivos, coercitivos e capazes de influenciar comportamentos, alinhando-se com os três requisitos formulados por Durkheim para caracterizar um fato social, neste caso, um fato social contemporâneo, sendo eles:

- **Exterioridade**: as normas, regras e comportamentos das redes sociais existem independentemente da vontade de cada indivíduo. Por exemplo, a cultura do cancelamento, a propagação de memes ou a pressão para se manter conectado são fenômenos que ultrapassam o controle individual e são impostos pelo ambiente social digital
- **Coercitividade**: as redes sociais exercem uma forte pressão sobre seus usuários, seja por meio de sanções sociais (como exclusão, críticas ou perseguição online), seja pela necessidade de adequação a padrões de comportamento, linguagem e aparência. Quem não segue essas normas pode sofrer consequências negativas, como isolamento ou perda de status social.
- **Generalidade**: os padrões de uso, os costumes e as tendências nas redes sociais são compartilhados por milhões de pessoas, tornando-se comuns a todos os usuários. Exemplos incluem a adoção de *hashtags*, desafios virais e formas de interação que se espalham rapidamente entre diferentes grupos.

Importante trazer à pesquisa que o Brasil não possui qualquer tecnologia equivalente em se tratando de redes sociais, o que desemboca em uma dependência estrutural dos usuários brasileiros, visto que a ferramenta já foi internalizada como parte da rotina dos usuários, dependência esta que não se deu por acaso, pelo contrário, incorporar um determinado produto ou serviço em uma sociedade, que para que esta se acostume e posteriormente criar uma relação de dependência é uma estratégia já experimentada outras vezes pelo capitalismo (Cassino; Silveira; Sousa 2021, p. 62).

Como sugestão de soluções para restabelecer o equilíbrio, sugere-se que a mudança de procedimento esteja em um passo antes do momento de consentir, na modalidade de aceite da plataforma, adaptando a legislação para que esta se adapte materialmente à dinâmica das redes sociais, de modo a permitir alguma margem de negociação dos usuários sobre seus dados podendo, por exemplo, exigir modelos alternativos de acesso como o acesso pago sem o tratamento de dados para fins de anúncio.

Acredita-se que o acúmulo de dados sobre os usuários extrapola os direitos de personalidade e que o ideal seria uma combinação de procedimentos, observados sob ótica individual e coletiva através de normas mais específicas sobre os dados obtidos através de inferências, mesmo nos casos em que as pessoas não possam ser identificadas.

Na ausência de identificação da pessoa, a proteção deve incidir sobre o grupo de pessoas perfiladas, já que a técnica, nas redes da Meta, não tem por finalidade descobrir a identidade, mas atribuir uma aos usuários, logo esse grupo social ao qual o usuário foi atribuído deve gozar de uma proteção, a exemplo do que já ocorre com outros grupos quando da aplicação de um direito difuso, por serem um grupo de pessoas indeterminadas, porém conectadas por uma situação de fato e/ou de direito.

Com base nos estudos de Bauman sobre a vigilância líquida, entende-se que, na sociedade atual, o consentimento do usuário nas redes sociais pode ser interpretado não como uma escolha genuinamente autônoma, mas como uma adaptação às exigências de exposição e participação social (Bauman, 2014).

Compartilhamos aqui no posicionamento de que o aceite nas redes sociais não é pautado em concordar e não concordar, mas em aceitar o serviço da forma em que este se encontra, ou ser excluído daquele ambiente, já que na forma *take it or leave it* não há margem de negociação entre usuário e plataforma.

2.4.1 Consentimento e a lacuna jurídica

Além dos dispositivos indicando a necessidade de consentimento, o MCI dedicou ainda outros 4 dispositivos para orientar o que seria um consentimento expresso²⁰, estabelecendo que as informações devem ser claras, completas e destacadas para preenchimento dos adjetivos em questão. Note que é necessário que o agente de tratamento,

²⁰Art. 7º, VI, VIII, IX e XI

neste caso, a rede social, informe quais os dados e como serão tratados, e sendo o caso de dados sensíveis o faça com uma maior carga participativa do usuário, ou seja, de maneira expressa (Bioni, 2019 apud Arruda 2021, p. 90).

Embora ainda sejam escassos os casos judiciais brasileiros que avaliem diretamente as situações de *profiling* em redes sociais, a jurisprudência do Superior Tribunal de Justiça (STJ) já reconheceu a incidência do Código de Defesa do Consumidor (CDC) em relações com plataformas digitais, reforçando a vulnerabilidade do usuário e a necessidade de transparência e controle sobre o tratamento de dados (STJ, REsp 1.316.921/RJ, 2012).

O entendimento pode ser estendido ao MCI, especialmente em casos de desvio de finalidade ou falta de clareza sobre o uso de dados para perfilização, como evidenciado em episódios internacionais como o caso Cambridge Analytica, que demonstram riscos concretos à privacidade e à autodeterminação informativa dos usuários (Brasil, STJ, 2012; Silva, 2024).

Todavia a problemática da relação consumidor x consentimento x *profiling*, está no fato de que em um primeiro momento a natureza dos dados tratados (apenas dados pessoais e/ou triviais) permite que o consentimento seja apenas informado, aquele que necessita de menor carga participativa.

Entretanto, como será demonstrado ao longo da pesquisa, a técnica de *profiling*, possibilita inferir dados pessoais e/ou pessoais sensíveis, a partir de dados triviais, como curtidas, interações e demonstrações de interesse — como, por exemplo, compartilhar um conteúdo ou comentar em uma postagem —, que permitem à empresa auferir dados a partir de inferências²¹, o que abre espaço para lacunas jurídicas procedimentais.

Em uma análise formal, atendendo ao requisito de ser um consentimento informado, as redes sociais possuem a legitimidade para tratar esses dados dentro dos limites expostos, qual seja, acessar os dados pessoais para fins de ofertar publicidade.

Entretanto, diversas pesquisas demonstram que, a partir do cruzamento desses dados, é possível inferir dados sensíveis. No entanto, a opacidade da dinâmica de tratamento impede que o usuário saiba com precisão se, e em que momento, tais dados foram extraídos, o que dificulta não apenas a atuação do consumidor, mas também de órgãos institucionais responsáveis por fiscalização e prevenção diante de eventuais violações dessa natureza²².

²¹ Informações obtidas através de inferências são informações sobre uma pessoa que não foram fornecidas diretamente por ela, nem captadas de forma explícita, mas sim deduzidas ou calculadas a partir da análise de outros dados pessoais, padrões de comportamento, interações digitais ou cruzamento de informações.

²² Os estudos que atestaram a inferência foram feitos por órgãos externos, nenhuma informação sobre tratamento de dados sensíveis dada pela própria plataforma foi encontrada

Outro ponto é sobre a incidência da LGPD, que como descrita no próprio nome, cuida da proteção de dados pessoais ou para formação do perfil comportamental de determinada pessoa natural, se identificada (art. 12 § 2º). A lei não faz menção a tratamento de dados não pessoais, ou dados para a formação de perfil comportamental em que a pessoa não seja identificada.

Ocorre que, quando se tratando de *profiling*, o usuário não precisa ser necessariamente identificado para que a intenção da plataforma seja bem-sucedida, já que basta que se enquadre em um perfil de consumo, logo é possível que a plataforma salve informações suficientes sobre um usuário, incluindo informações sensíveis sobre sexualidade e preferência política de forma a conseguir induzir seu comportamento sem necessariamente capturar dados como nome, Registro geral ou CPF.

Como resultado, a pesquisa realizada para este item, aponta para o cenário em que o consentimento dado pelo usuário como contrapartida para acessar a redes sociais não é o meio apropriado sob a ótica do princípio do livre desenvolvimento da personalidade, pois configura uma base legal meramente formal, pois de fato a escolha feita pelos usuários não é pautada unicamente na proteção de seus dados, mas no proveito social proporcionado pelas redes sociais, nos quais em uma balança o acesso ao convívio social e o desejo de não exclusão tende a permanecer.

2.5 Lei Geral de Proteção de Dados

Em 14 de agosto de 2018, após um longo tempo de trabalho, ajustes, adaptações e consultas públicas foi promulgada a Lei 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), inspirada pelo Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia.

A Lei n.º 13.709/2018 nasce com o intuito de regulamentar o tratamento de dados pessoais, por pessoas físicas ou jurídicas, públicas ou privadas, e institui seus fundamentos no artigo 2º: respeito à privacidade, a autodeterminação informativa, entre outros direitos fundamentais previstos na Constituição.

Todavia, a LGPD igualmente institui como fundamentos o desenvolvimento econômico, tecnológico e a inovação, de modo que não se estabelece uma hierarquia, entendendo a importância e necessidade de coexistência de ambos, o que reforça a dupla função do instituto (Bioni, 2019, p. 109)

Bioni (2019) analisa o contexto histórico das leis de proteção de dados sob a perspectiva de uma *dupla função*, conferindo um conjunto de direitos que confirmam segurança jurídica tanto ao cidadão como aos setores estatais e à economia privada, para simultaneamente possa garantir os direitos fundamentais dos cidadãos e o fomento do desenvolvimento econômico. (Bioni, 2019, p 108, grifo do autor). A seguir daremos início à análise dos dispositivos da LGPD afetos ao tema, iniciando pelo consentimento.

A hipótese do trabalho é que a técnica de perfilização praticada no ambiente das redes sociais da Meta Platform Inc. viola o livre desenvolvimento da personalidade previsto no art. 2º VII da LGPD.

Para que o tratamento de dados pessoais seja realizado, a LGPD determina em seu artigo 6º, uma série de princípios a serem observados: i. Finalidade, ii. Adequação, iii. Necessidade, iv. Livre acesso, v. Qualidade, vi. Transparência, vii. Segurança, viii. Prevenção, ix. Não discriminação, e x. responsabilização e prestação de contas, e visam a proteção do tratamento de dados em todo o seu ciclo de vida, desde a coleta até a eliminação (Bioni, 2021, p. 23-24).

Tais princípios têm a finalidade de garantir que todo tratamento de dados seja feito com transparência, nos termos do art. 9º, e no respeito à privacidade, começando pela necessidade de um propósito claro e explícito. Ou seja, o titular deve ser informado de forma detalhada sobre a razão pela qual seus dados estão sendo coletados e como serão utilizados, para que possa dar seu consentimento de forma livre e consciente.

Ponto importante sobre o princípio da transparência é a soberania do titular sobre seus dados. Nos termos do art. 18 o titular tem o direito de acessar relatórios e informações detalhadas sobre o tratamento de suas informações pessoais, podendo solicitar, sempre que achar necessário e quando cabível, atualizações, correções e a exclusão de seus dados (LGPD, 2018)

Dando sequência ao estudo dos princípios, temos o da Minimização, art. 6º da LGPD por este princípio a lei exige que apenas os dados indispensáveis sejam coletados, exigindo a coleta e o tratamento de dados pessoais devem ser limitados ao mínimo necessário para a finalidade específica para a qual foram coletados. Em teoria a empresa Meta deveria justificar o porquê cada dado é coletado e qualquer excesso na coleta ou retenção de dados pode ser visto como uma violação da legislação.

Quanto aos tipos de dados que estão sob a incidência da lei, a LGPD traz no 5º, sendo eles: dados pessoais, dados pessoais sensíveis, e dados anonimizados, este último estando sob

o crivo da lei apenas quando o processo de anonimização ao qual foram submetidos puder ser revertido.

A LGPD determina diferentes graus de proteção para dados pessoais e dados pessoais sensíveis, entendidos como uma categoria mais específica dos dados pessoais, como por exemplo, dados sobre origem racial ou étnica, de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual. artigo 5º, II, LGPD. Os termos de uso dos aplicativos analisados, Instagram e Facebook, não informam de maneira expressa se há ou não o tratamento de dados sensíveis em suas operações.

Da leitura dos termos de uso dos aplicativos da empresa Meta.Inc. Facebook e Instagram, segundo as informações da plataforma, verifica se que o objeto de tratamento da empresa são os dados pessoais, entretanto não foi possível identificar exatamente quais dados são captados e se dentre estes dados estão dados pessoais sensíveis, aparentemente a empresa utiliza um rol exemplificativo, vejamos:

Como nosso Serviço é financiado - Em vez de pagar pelo uso do Instagram, usando o serviço previsto nestes Termos, você reconhece que podemos veicular anúncios a você que empresas e organizações nos pagam para promover dentro e fora dos Produtos das Empresas da Meta. Usamos seus dados pessoais, como informações sobre atividades e interesses, para veicular anúncios que são mais relevantes para você (Meta, 2025).

Entretanto, em se tratando da técnica de perfilização, ou *profiling*, a dinâmica de tratamento é por natureza dedutiva,²³ ou seja, consiste justamente na combinação dos dados para a geração do perfil do consumidor, o que está diretamente ligado à inferência de dados, pois o consumidor fornece determinados dados de forma voluntária, mas a combinação dos dados fornecidos revela outros dados, não fornecidos pelo consumidor (Martins, 2019).

A LGPD confere maior proteção aos dados sensíveis com o intuito de coibir práticas discriminatórias em função de raça, cor, gênero entre outras condições que possam tornar os indivíduos socialmente vulneráveis. Vale mencionar que a divisão entre dados pessoais, anonimizados e sensíveis permite transmutação de classificação, permitindo uma migração de status a depender de como forem correlacionados, a exemplo do que ocorre com os dados

²³ O Regulamento Geral sobre Proteção de Dados no (GDPR) âmbito da União Europeia define *profiling* como: "Definição de perfis, qualquer forma de tratamento automatizado de dados pessoais que consiste em utilizar esses dados pessoais para avaliar certos aspectos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspectos relacionados com o seu desempenho profissional, a sua situação econômica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações"(Silva; Oliveira, 2021)

anonimizados, que a depender do agrupamento podem identificar informações sensíveis sobre um indivíduo (Brasil, 2018; Bioni, 2019).

Diante da ausência de informações mais precisas sobre o tratamento de dados sensíveis e sua respectiva forma de tratamento por parte da empresa Meta Platform Inc. traremos aos estudos casos recentes envolvendo a empresa para demonstrar a possibilidade de dados genéricos podem se transformar em dados sensíveis.

O primeiro exemplo é o estudo da Universidade de Cambridge que analisa as “curtidas” na rede social Facebook. A pesquisa conseguiu identificar com exatidão a porcentagem de usuários homossexuais, heterossexuais, brancos, negros, e suas preferências políticas, se republicana ou democrata. Segundo os resultados da pesquisa, a análise das curtidas dos usuários na rede social pode revelar, quase com exatidão, informações sensíveis dos usuários. O estudo demonstrou que registros digitais relativamente básicos do comportamento humano, podem ser usados para estimar de forma automática e precisa uma ampla gama de atributos pessoais (Kosinski; Stillwell; Graepel, 2013).

Após a análise dos dados pessoais e dados pessoais sensíveis, suas definições e características, passaremos à análise dos dados anonimizados, que a princípio, não estariam no escopo de proteção da Lei Geral de Proteção de Dados, exceto quando o processo de anonimização for revertido. “Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido”.

Sobre este tema traremos as discussões doutrinárias sobre os dados anonimizados, explorando os posicionamentos expansionistas e reducionistas, que tecem argumentos no sentido de quais seriam os limites de estruturação dos dados que permitiriam ou não identificar uma pessoa. Nos termos do artigo 12, § 2º da LGPD diz: “Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada (LGPD, 2019)

A ótica expansionista percebe dado pessoal ainda quando existir a inexatidão da identidade, pois acredita que mesmo quando se retira um dado individualizador, a exemplo de um CPF, seria possível o agregamento de outras informações, que se combinadas poderiam levar a identificação do usuário, de modo que em tese, todo usuário identificável é um usuário identificado em potencial. Visão esta que estaria em consonância com a LGPD, nos termos do

artigo 5º, I: “Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;” (Bioni, 2019).

Já a ótica reducionista acredita que para que a individualização ocorre apenas quando houver o reconhecimento do usuário de maneira exata, entendendo que se utilizadas técnicas para eliminar elementos identificadores de uma base de dados, como por exemplo, supressão, generalização, randomização e pseudo-anonimização, não haveria que se falar da incidência da lei de proteção de dados pessoais (Bioni, 2019).

A respeito, a Lei Geral de Proteção de dados adota a teoria expansionista, sob uma ótica mais ampla, reconhecendo como dado pessoal para além da pessoa natural identificada, mas também aquela identificável, entendimento reforçado e endossado no estudo técnico sobre anonimização de dados na LGPD: Análise jurídica emitido pelo órgão em 2023. (ANPD, 2023).

Bioni (2019) tece uma série de críticas sob o argumento de que o tratamento de dados para a formação de perfil comportamental, a depender do motivo e contexto em que a informação será aplicada, a identificação ou não do indivíduo não é o ponto relevante, pois a real intenção do tratamento não é identificar o usuário, mas de alguma forma influenciar a vida da pessoa que está atrás do dispositivo.

O autor ainda critica a formação do conceito direito de privacidade como um prolongamento da pessoa natural e não sugerindo que a proteção de dados seja alocada como um novo direito de personalidade bem como um novo arranjo de governança para que as normas abracem todo o tipo de processamento de dados, independentes de serem pessoais ou não, bastando que sujeite o indivíduo a uma coletividade ou a uma decisão automatizada.

Para Bioni (2019, p. 82) o foco não está no dado, mas no seu uso e as consequências desse uso na esfera do indivíduo, de modo que mesmo anonimizados podem comprometer o livre desenvolvimento da personalidade os dados forem utilizados para gerar decisões automatizadas sobre uma pessoa ou uma coletividade o tratamento estará dentro do escopo da proteção de dados pessoais.

Bioni compartilha da ideia de Miguel Reale, de que todo ser é eminentemente social e tem sua subjetividade desenvolvida a partir do seu relacionamento com o todo, propondo uma perspectiva mais ampla sobre o tema, nas palavras de Miguel Reale:

Nenhum conteúdo existencial é possível como ato singular isolado, o que decorre, aliás, do conceito mesmo de circunstância, que abrange, como

vimos, também a condicionalidade corpórea social do eu. (...), o que demonstra que nenhum eu é real a não ser em relação com outros eus, nenhuma subjetividade é tal senão com a intersubjetividade, ou socialidade, determinando e legitimando a pluralidade das ideologias (Reale, 2005 *apud* Bioni, 2019. p. 83)

Martins (2019) critica o consentimento, art.11 da LGPD, como a principal base legal para tratamento de dados, pois acredita que tal mecanismo em aplicação é atribuir ao usuário toda a responsabilidade pelo controle e coleta de dados sensíveis relativos a ele. Nas palavras de Martins:

Embora a princípio pareça contraintuitivo, confiar no consentimento como ferramenta de proteção do titular leva a uma menor proteção legal (SCHERMER et. al. 2014, LAZARO e MÉTAYER, 2015). Devido a enorme assimetria informacional entre controlador e titular (principalmente se tratando de inferências), no momento do consentimento o titular não tem como saber quais informações serão obtidas sobre ele, de forma que nenhuma escolha significativa e proteção efetiva seriam garantidas (Martins, 2019).

Como alternativa, Martins sugere que a base legal para o tratamento de dados sensíveis, incluindo os fornecidos pelos usuários e os de inferência, seja o legítimo interesse, pois desta maneira seria possível impor ao controlador a obrigação de gerar um relatório de impacto, constando os objetivos e consequências desse tratamento (Martins, 2019). Trazemos ao texto a observação de que a geração de relatórios de impacto para os casos em que o tratamento estiver fundamentado no interesse legítimo, possui previsão legal na LGPD, nos arts. 5º, XVII, art. 10 §3º e art. 38 da LGPD.

Entretanto, ao analisar qualitativamente o arcabouço normativo sobre proteção de dados, constatou-se uma deficiência da legislação brasileira sobre o tema, que não traz comandos específicos sobre a técnica de *profiling*/perfilização, nem mesmo a Lei Geral de Proteção de Dados, o que abre margens para excessos no tratamento dos dados bem como para desvios de finalidade.

Considerando que o objetivo desta seção foi levantar as questões jurídicas sobre *profiling* e proteção de dados, listamos abaixo as lacunas e pontos controversos constatados da exploração bibliográfica:

- ✓ **Eficácia do consentimento como base legal:** A análise da seção evidenciou que, embora o consentimento seja previsto pela LGPD como fundamento central para o tratamento de dados pessoais, sua efetividade é limitada diante da complexidade

das operações digitais e da assimetria informacional entre usuários e plataformas. O consentimento, frequentemente obtido em situações de “take it or leave it”, revela-se mais uma formalidade do que uma garantia substancial de autodeterminação informativa, o que suscita dúvidas sobre sua suficiência para proteger os direitos dos titulares (BONI, 2019).

- ✓ **Normas específicas sobre profiling/perfilização:** A seção destacou a ausência de dispositivos normativos detalhados sobre profiling na LGPD, o que resulta em lacunas regulatórias relevantes. Essa omissão dificulta a implementação de salvaguardas eficazes para decisões automatizadas e para a criação de perfis comportamentais, tornando o ambiente regulatório brasileiro menos protetivo diante dos riscos inerentes à perfilização em larga escala (BONI, 2019).
- ✓ **Proteção aos dados obtidos através de inferência:** No tocante aos dados inferidos, foi identificado que a LGPD não disciplina de modo claro o tratamento dessas informações, permitindo que dados sensíveis sejam deduzidos a partir de dados aparentemente triviais sem o conhecimento do titular. Essa lacuna amplia os riscos à privacidade e à dignidade dos indivíduos, evidenciando a necessidade de regulamentação mais precisa para garantir a proteção efetiva dos titulares (ANPD, 2023; BONI, 2019).
- ✓ **Proteção de dados de pessoas não identificáveis conectadas por uma situação de fato:** Por fim, a seção apontou que a proteção conferida pela LGPD aos dados de pessoas não identificáveis, mas conectadas por uma situação de fato, é insuficiente. Mesmo sem identificação direta, o agrupamento e análise desses dados podem gerar impactos coletivos e decisões discriminatórias, demandando uma abordagem normativa mais abrangente para assegurar os direitos fundamentais dos titulares diante das novas dinâmicas do tratamento automatizado (Boni, 2019; ANPD, 2023).

2.6 O papel da Agência Nacional de Proteção de dados – ANPD

A Autoridade Nacional de Proteção de Dados (ANPD) é uma autarquia de natureza especial prevista no art. 55- A da LGPD,²⁴ vinculada ao Ministério da Justiça e Segurança Pública, responsável por selar, garantir e fiscalizar o cumprimento da LGPD no Brasil, figurando como um agente interlocutor para as questões de regulação e cumprimento de proteção de dados promovendo uma interpretação e execução uniforme dos comandos da LGPD (Centro de Direito, Internet e Sociedade do Instituto Brasiliense de Direito Público CEDIS-IDP²⁵, 2020; ANPD, 2024).

As prerrogativas da ANPD abrangem competências administrativas, normativas e sancionatórias, que permite ao órgão, editar normas e procedimentos sobre proteção de dados, fiscalizar e aplicar sanções administrativas (como advertências, multas e bloqueio de dados), supervisionar o tratamento de dados pessoais, deliberar sobre a interpretação da LGPD, regular ou proibir o compartilhamento de dados sensíveis para fins econômicos, além de atuar em processos administrativos e judiciais de forma independente (ANPD, 2022)

O caso mais recente da ANPD envolvendo a empresa Meta.Inc ocorreu em 2024, quando a ANPD determinou, através de uma medida preventiva, a suspensão do uso de dados de usuários brasileiros do Facebook e Instagram pela Meta para fins de treinamento de um novo produto da empresa, no caso uma inteligência artificial generativa (ANPD, 2024).

A decisão foi motivada pela falta de transparência da Meta quanto à finalidade do tratamento de dados, pelo uso de base legal inadequada (legítimo interesse) para tratar dados sensíveis, e pelos riscos à privacidade de grupos vulneráveis, como crianças e adolescentes. A medida incluiu multa diária em caso de descumprimento e exigiu a exclusão dos dados já coletados (ANPD, 2024).

A medida preventiva foi suspensa, após o Conselho Diretor aprovar um Plano de Conformidade, do qual constam diversas medidas que deverão ser implementadas pela empresa com vistas à adequação de suas práticas, permitindo que a empresa retornasse com as atividades de treinamento de inteligência artificial generativa (ANPD, 2024).

Entretanto, chama atenção o fato de a ANPD ter provado que a empresa utiliza-se da técnica de “*opt out*”, bastante criticada pela doutrina brasileira, que tece críticas quanto à

²⁴ Art. 55-A. Fica criada a Autoridade Nacional de Proteção de Dados (ANPD), autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal.

²⁵ CEDIS-IDP-Centro de Direito, Internet e Sociedade do Instituto Brasiliense de Direito Público.

imputação ao usuário de ter que se opor sob pena de o silêncio importará em anuênciam tácita. Parte da doutrina entende que o formato mais adequado a ser apresentado aos consumidores seria a opção “*opt in*”, ou seja, o silêncio do usuário importaria em negativa e a plataforma só capta os dados após o usuário consentir de forma expressa (Mendes, 2014).

Mendes compartilha do posicionamento de que o modelo *opt out* não é compatível com o requisito de consentimento expresso e, por consequência, apenas o modelo *opt in* é capaz de conferir validade a um consentimento legítimo (Mendes, 2014).

Em relação à prática de *profiling* e decisões automatizadas em redes sociais, a autoridade tem se manifestado de forma cautelosa e protetiva. A ANPD defende a necessidade de transparência quanto aos critérios utilizados em decisões automatizadas conforme o art. 20 da LGPD, permitindo ao titular o direito de revisão dessas decisões e a mitigação de riscos de discriminação decorrentes do uso de algoritmos e perfis comportamentais (ANPD, 2023).

A ANPD também ressalta que o tratamento massivo de dados, mesmo que trivial, pode levar à inferência²⁶ de dados sensíveis, exigindo salvaguardas adicionais e respeito aos princípios da LGPD, como finalidade e necessidade (Martins, 2019; ANPD, 2023).

Sobre as inferências, Pedro Bastos Lobo Martins, alerta que a categoria de dados pessoais sensíveis, em um primeiro momento pode parecer algo muito específico, mas quando se trata de proteção de dados as relações são sempre dinâmicas e contextuais, o que na prática demanda de uma análise de acordo com o caso concreto e a atividade de tratamento pretendida para constatar se um dado é ou não sensível. Martins pontua ainda que, com a difusão da capacidade de inferência da informação dos titulares qualquer dado pessoal poderá ser categorizado como dado pessoal sensível. Nas palavras do autor:

Em um breve exemplo: ao informar seu nome para reserva de um restaurante, provavelmente esse dado não será considerado sensível. Por outro lado, se um imigrante, ao contratar um plano de saúde, preenche um formulário com seu nome, que facilmente identifica sua origem étnica e isso afeta o preço do serviço oferecido, **seu nome pode ser considerado um dado sensível.** (Grifo do autor) (Martins, 2019).

Neste sentido, O pesquisador de inteligência artificial do Instituto Universitário Europeu (EUI), Marco Almada, destaca a importância de a ANPD estabelecer critérios mais

²⁶Inferências, no contexto da proteção de dados e da LGPD, são informações sobre uma pessoa que não foram fornecidas diretamente pelo titular, mas que são deduzidas ou criadas a partir do processamento e análise de outros dados pessoais

precisos sobre o uso de decisões automatizadas no tratamento de dados pessoais, pois acredita que o art. 20 da LGPD abre margem para uma série de interpretações, necessitando de parâmetros objetivos para evitar situações discriminatórias, nas palavras de Marco Almada.

Dentro desta moldura, a ANPD possui a discricionariedade necessária para estabelecer regras que promovam a construção e uso de sistemas automatizados cujas decisões sejam efetivamente passíveis de revisão, seja ela feita ou não por humanos. Este estabelecimento pode ocorrer tanto através do uso de instrumentos normativos quanto por meios não-vinculantes, como o estímulo à criação por particulares de padrões para o projeto e uso de sistemas capazes de tomar decisões unicamente baseadas no processamento automático de dados (Almada, 2019. p. 19).

Todavia, da leitura dos termos de uso e políticas de privacidade dos aplicativos Facebook e Instagram não foi encontrado qualquer menção à possibilidade de o usuário rever o perfil que lhe foi atribuído, seus respectivos critérios ou a possibilidade de revisão das decisões automatizadas com base nestes.

De novembro de 2024 a dezembro de 2025 a ANPD promoveu uma tomada de subsídios²⁷, a fim de fomentar o debate técnico sobre o tratamento automatizado de dados pessoais, entendendo como tratamento automatizado aquele que ocorre quando um sistema, programa ou tecnologia, incluindo sistemas algorítmicos ou de inteligência artificial, realiza operações com dados pessoais sem intervenção humana significativa envolvendo coleta, armazenamento, análise e tomada de decisões baseadas em critérios predefinidos, como classificação, avaliação, aprovação ou rejeição, entre outros.

Ocorre que o *profiling* (perfilamento) é uma modalidade específica de tratamento automatizado, que consiste na análise e avaliação de dados pessoais para criar perfis que permitem prever comportamentos, preferências ou características dos titulares, influenciando decisões automatizadas ou semiautomatizadas. Assim, o profiling é um tratamento que utiliza dados pessoais para fins de avaliação individual ou coletiva com efeitos supraindividuais, podendo afetar grupos e a sociedade, e que sua regulação deve contemplar salvaguardas

²⁷ Tomada de Subsídios é um procedimento consultivo que tem como objetivo reunir contribuições detalhadas de especialistas, organizações sociais, empresas privadas, órgãos governamentais e demais interessados para fundamentar e aprimorar a elaboração de normas e regulamentações relacionadas à proteção de dados pessoais. Diferentemente da Consulta Pública, a Tomada de Subsídios não é obrigatória, mas permite um diálogo técnico aprofundado, com a apresentação de informações técnicas, estudos de caso e práticas internacionais que enriquecem o processo regulatório. Esse mecanismo auxilia a ANPD a identificar riscos, desafios e melhores práticas, especialmente em temas complexos como inteligência artificial, decisões automatizadas e proteção de dados sensíveis (BRASIL, ANPD, 2024).

específicas, como transparência, direito à explicação e avaliações de impacto (MARTINS, 2021, p. 105-108; 121-132; 146-177).

Todavia a ANPD tem tratado o tema de forma mais genérica, considerando em um primeiro momento as decisões automatizadas de forma mais genéricas, sem setorizar as discussões, de modo que não há, ao tempo desta pesquisa um posicionamento específico sobre perfilização, tampouco sobre a prática aplicada às redes sociais.

A GDPR (Regulamento Geral de Proteção de Dados da União Europeia) legislação que inspirou a LGPD, tratou o tema da perfilização (*profiling*) de forma expressa e detalhada, definindo no art. 4º, como qualquer forma de tratamento automatizado de dados pessoais que consista na utilização desses dados para avaliar aspectos pessoais de uma pessoa física, incluindo os perfis formados a partir de inferências mesmo quando não revelem diretamente a identidade da pessoa (Regulamento (UE) 2016/679, art. 4º, nº 4).

Diferentemente da GDPR, a LGPD, por sua vez, não reproduz explicitamente essa definição específica para *profiling*, apesar de mencionar a perfilização no art. 12 § 2º, porém não incluiu no escopo da lei os dados anonimizados, e sobre os dados obtidos através de inferências, permanecem no escopo da lei apenas aqueles que permitam a identificação (Brasil, 2018).

Essa ausência gera desafios para a regulação no Brasil, pois limita a abrangência da proteção e dificulta o controle sobre práticas algorítmicas que utilizam inferências para criar perfis, potencialmente comprometendo direitos fundamentais. Martins (2019) argumenta que essa lacuna normativa exige uma interpretação hermenêutica que considere os princípios constitucionais do livre desenvolvimento da personalidade e da autodeterminação informativa, ampliando o escopo da proteção para abranger também os dados inferidos e os efeitos supraindividuais do *profiling* (Martins, 2021, p. 132-146).

Martins ressalta que a regulação do *profiling* deve ir além da mera reprodução da GDPR, incorporando um enfoque substantivo que garanta transparência, o direito à explicação e a realização de avaliações de impacto algorítmico, conforme recomendam documentos oficiais da ANPD e estudos internacionais (Martins, 2021, p. 146-177; ANPD, 2024).

A seção 2 apresentou uma análise da construção jurídico-normativa das leis de proteção de dados no Brasil, destacando a evolução legislativa e os desafios impostos pela era da informação. Foram abordados os fundamentos constitucionais, o Código de Defesa do Consumidor, o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD),

evidenciando lacunas e pontos controversos, como a eficácia do consentimento, a ausência de normas específicas sobre profiling e a proteção de dados obtidos através de inferência inferidos.

Os resultados indicaram que, embora o arcabouço jurídico brasileiro ofereça subsídios mínimos para a proteção de dados, ainda carece de regulamentação mais específicas sobre a prática e perfilização, especialmente no contexto das redes sociais. A análise também revelou a necessidade de maior transparência por parte das plataformas, além de uma atuação mais robusta da ANPD para mitigar riscos e garantir a proteção dos direitos fundamentais.

3 O LIVRE DESENVOLVIMENTO DA PERSONALIDADE E A PROTEÇÃO DE DADOS

Uma vez que a ideia desta seção é demonstrar a construção jurídica sobre a proteção e dados sob perspectiva do direito ao livre desenvolvimento e da autodeterminação informativa, faz-se relevante trazer os precedentes jurisprudenciais que inauguraram o conceito de proteção de dados como se conhece hoje, por inaugurar o que Mayer-Schonberger chama de terceira geração de proteção de dados (Mendes, 2014).

3.1 Precedentes históricos sobre direito ao livre desenvolvimento da personalidade e autodeterminação informativa.

3.1.1 O Julgamento da Lei do Censo de 1983

A primeira geração de leis de proteção de dados surge na Alemanha na década de 70, motivada pelas burocracias governamentais, que dependiam de um grande volume de dados dos cidadãos para serem alcançadas, como por exemplo: a iniciativa do estado alemão de conectar bancos de dados municipais, estaduais e a proposta do parlamento sueco em 1960 de fundir os dados de informações fiscais com os dados civis e os dados do censo (Mendes, 2014).

Em resposta a este movimento foram criadas leis como: a Leis do Estado alemão de Hesse (1970) a lei da Suécia (1973), o estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977).

Ocorre que ao tempo em que foram editadas, as leis de primeira geração tinham como características priorizar os procedimentos burocráticos, criando regras, rotinas, exigências formais e não a efetiva proteção dos direitos fundamentais dos titulares desses dados como, privacidade, liberdade, autodeterminação informativa e o real controle sobre suas informações pessoais, o que fez com que as leis precisassem se moldar para garantir efetividade material, dando início assim às leis de segunda geração (Mendes, 2014).

A segunda geração surge com a característica de priorizar o direito à privacidade ao em vez de procedimentos, as leis são pensadas sob uma perspectiva da liberdade individual

dos usuários de forma ampla, abraçando assim a privacidade informacional, como exemplo, as leis da Áustria, França, Dinamarca e Noruega (Mendes, 2014).

A segunda geração de leis percebe uma inclinação para a pulverização das informações dos usuários ao redor do mundo por diferentes empresas, públicas e privadas, conectadas em rede, o que motivou a população desses países a lutar por direitos mais efetivos de preservação da privacidade. Característica marcante desta segunda geração de leis foi a ampliação no âmbito institucional, expandindo os poderes das autoridades administrativas responsáveis pela proteção de dados (Mendes, 2014).

Outro ponto relevante é que a segunda geração de normas de proteção de dados, foi a primeira a trazer questionamentos sobre o custo social do exercício de direito à privacidade, apontando a dualidade dos cidadãos de, por um lado exercerem sua privacidade e liberdade informacional e por outro a possibilidade de exclusão social, como pontua Mendes:

Por um lado, no âmbito do Estado Social, é muito difícil assegurar-se a liberdade informacional sem comprometer as funções dessa complexa burocracia que necessita de dados dos cidadãos para planificar. Por outro, também na relação entre privados é difícil se verificar o exercício do direito à privacidade informacional, na medida em que tal exercício poderá impedir o acesso ao indivíduo à determinadas facilidades do mercado de consumo, que o fornecedor está disposto a conceder somente em troca de suas informações pessoais (Mendes, 2014, p. 685).

A terceira geração das normas de proteção de dados é marcada pela decisão do Tribunal Constitucional alemão, em 1983, ao analisar a lei do censo e declara lá parcialmente inconstitucional sob o fundamento da autodeterminação informativa e tem como principal característica o aumento da carga participativa do cidadão no processo de controle sobre seus dados, entendendo que a conexão entre os cidadãos e seus dados deve ser contínua e não apenas no momento do consentimento (Mendes, 2014).

O caso versava sobre a coleta de dados pessoais da população para fins de recenseamento, necessários para a elaboração de políticas públicas. Entretanto a lei previa a possibilidade de compartilhamento desses dados com outras repartições públicas para fins de administrativos.

Importante ressaltar o contexto fático da decisão, que levou em consideração o processamento automatizado de cruzamento dos dados. O tribunal entendeu que a conexão entre diferentes bancos de dados por parte do estado abriria margem para a obtenção de novas informações sobre os usuários através de inferências, conforme trecho do julgado:

Hoje, com ajuda do processamento eletrônico de dados, informações detalhadas sobre relações pessoais ou objetivas de uma pessoa determinada ou determinável (dados relativos à pessoa [cf. § 2 I BDSG – Lei Federal de Proteção de Dados Pessoais]) podem ser, do ponto de vista técnico, ilimitadamente armazenadas e consultadas em qualquer momento, a qualquer distância e em segundos. Além disso, podem ser combinadas, sobretudo na estruturação de sistemas de informação integrados, com outros bancos de dados, formando um quadro da personalidade relativamente completo ou quase, sem que a pessoa atingida possa controlar suficientemente sua exatidão e seu uso. Com isso, ampliaram-se, de maneira até então desconhecida, as possibilidades de consulta e influência que podem atuar sobre o comportamento do indivíduo em função da pressão psíquica causada pela participação pública em suas informações privadas (Martins, 2016).

Tal dispositivo foi considerado parcialmente inconstitucional pelo tribunal europeu, sob o fundamento de ser contrário ao livre desenvolvimento da personalidade, já previsto de forma expressa na Constituição alemã, no artigo 2º, à época do julgamento, art. 2º “*todos tem o direito ao livre desenvolvimento da sua personalidade, desde que não violem os direitos de outros e não atentem contra a ordem constitucional ou a lei moral*” (Alemanha, 1949).

Ao final, o Tribunal Constitucional Federal entendeu que a coleta e o tratamento de dados pessoais deveriam estar submetidos a normas procedimentais, destinadas a restringir o compartilhamento dessas informações e a implementar salvaguardas que reduzissem os riscos à esfera de direitos dos cidadãos.

O julgado se mostra relevante por reconhecer o direito de autodeterminação informativa e consolidar uma visão flexível do direito de personalidade, considerando formulações que guardem relação com a materialidade, entendendo a atualização e adaptação das leis como um dever estatal, rompendo com a lógica tradicional de privacidade apenas como um direito de sigilo e preservação da intimidade (Mendes, 2020).

O tribunal reconheceu que o compartilhamento entre as instituições violaria a finalidade para o qual os dados inicialmente foram coletados levando em consideração o processo aos quais os dados são submetidos, ampliando a análise do sentido de legalidade para além do consentimento e abrangendo a aplicação da lei, O que fez com que o caso se tornasse referência em matéria de proteção de dados e Direito de Personalidade (Martins, 2021).

O tribunal entendeu que a transferência indiscriminada desses dados violava o direito ao livre desenvolvimento da personalidade, protegido pelo artigo 2º, parágrafo 1º, em conjunto com o artigo 1º, parágrafo 1º da Lei Fundamental, e criou o direito à

autodeterminação informativa, conferindo ao indivíduo o poder de decidir sobre a divulgação e o uso de suas informações pessoais.

A conjugação teórica não apenas ampliou o escopo de proteção dos direitos da personalidade, mas também cria um ambiente propício para a evolução jurisprudencial que acompanha as transformações sociais e tecnológicas, tal qual a visão monista sobre direitos da personalidade que será analisada mais a frente em tópico próprio.

3.1.2 O Caso IBGE

No Brasil, destaca-se o caso IBGE, cuja análise revela pontos de convergência com o emblemático precedente alemão de 1983. A partir deste momento, a pesquisa concentrar-se-á em analisar os contornos jurídicos das Ações Diretas de Inconstitucionalidade (ADI), em que o Supremo Tribunal Federal avaliou a constitucionalidade dos dispositivos da Medida Provisória 954.

Em abril de 2020, diante do cenário de emergência sanitária provocado pela pandemia de COVID-19, a Presidência da República editou a Medida Provisória 954, que estabelecia a obrigatoriedade de compartilhamento de dados pessoais entre as empresas de telefonia e o Instituto Brasileiro de Geografia e Estatística (IBGE). A medida tinha como objetivo viabilizar a realização da Pesquisa Nacional por Amostra de Domicílios Contínua (PNAD) remotamente, evitando a exposição de entrevistadores e entrevistados aos riscos de contágio (Brasil, 2020).

Para possibilitar a condução das entrevistas por telefone, a Medida Provisória determinou que as operadoras de telefonia fornecessem ao IBGE informações como nome, número de telefone e endereço de todos os seus clientes. Entretanto a iniciativa suscitou intensos debates sobre a proteção de dados pessoais e o equilíbrio entre o interesse público em tempos de crise e os direitos fundamentais à privacidade e à autodeterminação informativa.

Em um primeiro momento a medida se mostrava, razoável diante da urgência e aparentemente estava em conformidade com a LGPD, que se encontrava em período de *vacatio legis*:

Art. 2º, § 1º Os dados de que trata o caput serão utilizados direta e exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares. Art. 3º Os dados compartilhados:

I - Terão caráter sigiloso; II - serão usados exclusivamente para a finalidade prevista no § 1º do art. 2º; e III - não serão utilizados como objeto de certidão ou meio de prova em processo administrativo, fiscal ou judicial, nos termos do disposto na Lei nº 5.534, de 14 de novembro de 1968.

§ 1º É vedado à Fundação IBGE disponibilizar os dados a que se refere o caput do art. 2º a quaisquer empresas públicas ou privadas ou a órgãos ou entidades da administração pública direta ou indireta de quaisquer dos entes federativos.

§ 2º A Fundação IBGE informará, em seu sítio eletrônico, as situações em que os dados referidos no caput do art. 2º foram utilizados e divulgará relatório de impacto à proteção de dados pessoais, nos termos do disposto na Lei nº 13.709, de 14 de agosto de 2018 (Brasil, 2020).

A Medida provisória previa ainda o descarte dos dados ao fim da emergência sanitária em um prazo máximo de 30 dias, de modo que parecia atender aos requisitos de razoabilidade e finalidade.

Todavia a Medida foi objeto de questionamento no STF através das Ações Diretas de Inconstitucionalidade: A ADI 6387 foi proposta pelo Partido Socialista Brasileiro (PSB), a ADI 6388 pelo Partido dos Trabalhadores (PT), a ADI 6389 pelo Partido Democrático Trabalhista (PDT), a ADI 6390 pelo Partido Socialismo e Liberdade (PSOL), e a ADI 6393 pela Confederação Nacional das Profissões Liberais (CNPL)²⁸, que questionavam a compatibilidade da Medida com os direitos fundamentais da dignidade da pessoa humana, privacidade, autodeterminação informativa, sigilo de correspondências e comunicações (Brasil, 2020).

Os proponentes compunham-se de partidos políticos e entidades de classe e buscavam o submeter a MP ao controle concentrado de constitucionalidade²⁹. Em comum, os impetrantes alegaram que a Medida Provisória nº 954/2020 violava direitos fundamentais assegurados pela Constituição Federal, especialmente a dignidade da pessoa humana (art. 1º, III), o direito à privacidade (art. 5º, X), à inviolabilidade das comunicações (art. 5º, XII) e à

²⁸ Conforme o artigo 103 da Constituição Federal de 1988, possuem legitimidade para propositura de Ação Direta de Inconstitucionalidade os partidos políticos com representação no Congresso Nacional e as confederações sindicais ou entidades de classe de âmbito nacional. No caso da MP 954/2020, além dos partidos PSB, PT, PDT e PSOL, também foi autora da ADI 6393 a Confederação Nacional das Profissões Liberais (CNPL), entidade de classe com atuação em todo o território nacional. A legitimidade dessas entidades foi reconhecida pelo STF nos autos das respectivas ações (Brasil, 1988; STF, 2020).

²⁹ O controle concentrado de constitucionalidade é o modelo pelo qual se verifica a compatibilidade de normas com a Constituição por meio de ações propostas diretamente ao Supremo Tribunal Federal, como as Ações Diretas de Inconstitucionalidade (ADIs) e Ações Declaratórias de Constitucionalidade (ADCs). Diferentemente do controle difuso, exercido por qualquer juiz ou tribunal no caso concreto, o controle concentrado possui efeitos vinculantes e erga omnes, tendo natureza objetiva, pois visa à proteção da ordem constitucional, e não apenas à solução de um conflito individual (Barroso, 2018).

autodeterminação informativa, decorrentes do princípio da proteção da personalidade (Doneda, 2020; Monteiro, 2020).

Argumentou-se que a exigência de repasse imediato de dados de usuários por parte das empresas de telecomunicações, sem consentimento dos titulares, finalidade clara ou mecanismos de salvaguarda, configurava um grave retrocesso na proteção de dados pessoais e uma ameaça à esfera privada dos cidadãos.

De início a Medida teve sua eficácia deferida pelo voto da ministra Rosa Weber. No entanto, posteriormente o plenário do STF suspendeu a eficácia da medida, ratificando a decisão por 10 votos 1. A corte reconheceu de forma unânime a importância da Pesquisa Nacional por Amostra de Domicílios - PNAD e a relevância social do IBGE, entretanto o entendimento foi de que na ponderação de interesses do caso concreto a proteção de dados deveria prevalecer (Brasil, 2020).

A fundamentação adotada pelo Supremo Tribunal Federal assume especial relevância, configurando como um paralelo histórico à decisão do Tribunal Constitucional Alemão previamente analisada, ao reforçar a centralidade da proteção de dados pessoais e elevá-la à condição de direito fundamental autônomo e dinâmico.

Da análise das jurisprudências estudadas anteriormente pode se concluir que a proteção de dados deve ser revisitada de tempos em tempos, para que possa se adequar ao novo momento social e tecnológico. As decisões apontam para uma inclinação do judiciário de interpretar os direitos sobre proteção de dados de forma ampla e sob uma perspectiva constitucional e demonstram a tendência a interpretar a proteção de dados como um direito autônomo que não se restringe à lógica de não intervenção do estado na vida privada, mas como um verdadeiro direito de personalidade e autoafirmação.

3.2 A personalidade como um direito fundamental

Uma vez que o objeto da pesquisa cuida de analisar a técnica de perfilização/*profiling* sob a ótica do livre desenvolvimento da personalidade, enquanto um fundamento da LGPD art. 2º, VII, este item cuidará de apresentar os conceitos de personalidade, identidade e sua relação com livre desenvolvimento da personalidade e a autodeterminação informativa, entendendo como tais institutos se relacionam e como a doutrina e o judiciário brasileiro tem entendido o tema.

Os direitos de personalidade têm como objeto as expressões da personalidade, destinado a garantir o desenvolvimento físico e moral de sua existência, em geral considerados extrapatrimoniais inalienáveis, impenhoráveis, imprescritíveis, indisponíveis, inatos, absolutos, necessários, vitalícios, inerentes à pessoa, irrenunciáveis e não se extinguem com o tempo, de caráter absoluto e oponível *erga omnes*, ou seja, impõem a toda a coletividade o dever geral de abstenção, impedindo que terceiros interfiram no exercício desses direitos pelo titular (Brasil, 2002).

Inerentes à pessoa humana, os direitos da personalidade manifestam-se em toda a sua existência. Iniciando com o nascimento com vida, resguardados os direitos do nascituro. Cabe destacar que existem discussões doutrinárias sobre a aplicação desses direitos antes do nascimento e mesmo após a morte, como a proteção ao nascituro ou à memória do falecido. Contudo essas questões não serão aprofundadas neste trabalho para evitar distanciamento do objeto de análise proposto.

Outra discussão sobre os direitos de Personalidade é quanto à abrangência e forma de proteção: a qual se divide em 2 correntes principais, a monista e a pluralista. Uma entende tais direitos como uma série de direitos distintos e autônomos entre si e a outra defende que existe um único direito geral que engloba a pessoa humana em suas múltiplas dimensões, reunidas em uma unidade.

Para a teoria monista, existe um único direito geral da personalidade, de natureza abstrata e abrangente, do qual derivam todas as demais manifestações, assegurando a proteção da individualidade da pessoa em seus múltiplos aspectos e permitindo a tutela jurídica mesmo diante de novas situações, ainda que não estejam expressamente previstas em lei (Pinto, 2024).

Ao eleger a dignidade da pessoa humana como fundamento da República, a Constituição brasileira introduz uma cláusula geral de proteção da personalidade, o que aproxima o sistema desta visão em nível constitucional.

Por outro lado, a teoria pluralista defende a existência de diversos direitos de personalidade autônomos, cada qual relacionado a um aspecto específico da pessoa, como a integridade física, psíquica e moral, sendo necessário que estejam tipificados na legislação para que recebam proteção jurídica, a exemplo do que acontece no código Civil brasileiro (Pinto, 2024).

Embora o Código Civil traga em seus artigos 11 a 21 uma enumeração dos direitos de personalidade, o que se relaciona, ao menos do ponto de vista formal, com a teoria pluralista,

a doutrina e a jurisprudência brasileira reconhecem que tal rol não é exaustivo, permitindo a ampliação da proteção conforme as demandas sociais e o princípio constitucional da dignidade da pessoa humana. Sendo assim o sistema jurídico brasileiro adota a teoria pluralista no âmbito infraconstitucional, mas reconhece elementos da teoria monista na interpretação constitucional, indicando uma convivência das duas teorias (Filippo, 2009).

Roxana Cardoso Brasileiro Borges (2020), tal qual a teoria monista, entende que os direitos da personalidade não constituem uma lista fechada de prerrogativas, mas sim um microssistema aberto e dinâmico, fundamentado na dignidade da pessoa humana, conforme previsto no artigo 1º, inciso III, da Constituição Federal.

A autora destaca que a proteção desses direitos se dá por meio de uma cláusula geral, que permite o reconhecimento de novas situações e interesses existenciais relevantes, mesmo que não estejam expressamente previstos no ordenamento jurídico. Dessa forma, a tutela dos direitos da personalidade acompanha a evolução social e cultural, possibilitando uma interpretação expansiva e adequada às necessidades concretas da pessoa humana, em consonância com os princípios constitucionais (Borges, 2020).

Ao examinar o inciso III, do artigo 1º, da Constituição Federal³⁰, observa-se que os direitos da personalidade, no nosso sistema jurídico, configuram-se simultaneamente como uma lista aberta de direitos e como uma cláusula geral voltada à proteção da dignidade da pessoa humana. No ordenamento brasileiro, as noções de “lista aberta de direitos” e “direito geral da personalidade” não se excluem ou se anulam, possuindo ambas as iguais importância, permitindo em determinados casos, uma ampliação da proteção da pessoa em seus diversos aspectos de dignidade, ainda que tais direitos não estejam explicitamente previstos na legislação, ou seja, independentemente de sua tipificação legal (Borges, [s.d.]).

Percebe-se que de maneira geral, no Brasil prevalece a teoria monista, pois foi com base em uma interpretação mais ampla do Direito de Personalidade que surgiram os primeiros precedentes, reconhecendo o direito ao livre desenvolvimento e a autodeterminação informativa, que possibilitaram a evolução do direito contemporâneo de forma a abranger novos aspectos da personalidade, que por consequência geraram novos direitos passíveis de tutela.

³⁰Art. 1ºA República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: III - a dignidade da pessoa humana;

Neste item, demonstrou-se que o direito de personalidade a jurisprudência e a doutrina brasileiras adotam uma interpretação de cunho monista, especialmente no âmbito constitucional, permitindo a tutela de novas dimensões da personalidade, o que inclui o livre desenvolvimento da personalidade e a autodeterminação informativa, permitindo a efetivação de novos direitos, mesmo diante de contextos ainda não tipificados pelo legislador, possibilitando a abrangência da tutela jurídica à pessoa humana.

3.3 O Direito ao Livre Desenvolvimento da Personalidade – privacidade e proteção de dados nas redes sociais

Neste item, será analisado o direito ao livre desenvolvimento da personalidade à luz da proteção de dados, considerando sua relevância para a tutela dos direitos individuais frente às novas tecnologias e ao tratamento massivo de informações pessoais, que ganharam contornos ainda mais relevantes após a entrada em vigor da Lei Geral de Proteção de Dados.

Historicamente os direitos da personalidade no Código Civil brasileiro estiveram marcados por uma visão patrimonialista, na qual esses direitos eram compreendidos como uma espécie de direitos subjetivos vinculados a bens jurídicos, aproximando-se da lógica dos direitos patrimoniais, contudo, com o avanço da sociedade surgiram novos desafios, dos quais um olhar puramente patrimonial não seria capaz de solucionar, especialmente no que diz respeito ao fluxo e ao controle dos dados pessoais. (Fachin, 2007; Silva; Dinallo, 2021).

Essa abordagem limitava a compreensão da personalidade a uma tutela restrita de interesses individuais, muitas vezes sem considerar sua dimensão existencial e intrínseca à dignidade da pessoa humana. Essa perspectiva se mostrou insuficiente para abarcar a complexidade e a profundidade dos direitos da personalidade, que transcendem a mera propriedade ou titularidade de bens, envolvendo aspectos extrapatrimoniais, essenciais da identidade e autonomia do indivíduo (Fachin, 2007; Silva; Dinallo, 2021).

Especialmente a partir do século XX, A doutrina brasileira, passou a questionar essa visão restrita, defendendo a necessidade de uma abordagem mais ampla e constitucionalizada dos direitos da personalidade, que os reconheça como direitos fundamentais, indisponíveis e inerentes à pessoa humana em sua totalidade (Fachin, 2007).

Luiz Edson Fachin (2007), jurista brasileiro e ministro do Supremo Tribunal Federal, endossa o posicionamento, de que os direitos da personalidade devem ser compreendidos à luz dos princípios constitucionais, especialmente o da dignidade da pessoa humana, e que sua

proteção ultrapassa o campo do direito patrimonial, envolvendo também dimensões subjetivas e sociais.

Essa evolução doutrinária é fundamental para compreender a atual valorização do livre desenvolvimento da personalidade, tema central desta seção, especialmente no contexto da proteção de dados pessoais, onde a autonomia e a identidade do indivíduo ganham novas dimensões e desafios.

No Brasil, a Lei Geral de Proteção de Dados foi o primeiro instituto a incluir o livre desenvolvimento da personalidade de maneira expressa, elencando tal direito no art. 2º, como fundamento da lei. Antes da edição da LGPD era admitido como um princípio implícito, utilizado como chave interpretativa da legislação de proteção de dados. (Martins, 2021).

O livre desenvolvimento da personalidade tem como principais elementos a proteção da individualidade, garantindo indivíduos autonomia para buscar a construção dos elementos que o identifique de forma livre e autônoma. Entretanto, apesar de seu caráter subjetivo, possui necessariamente uma dimensão social, que necessita da interação com outras pessoas como contexto para que o desenvolvimento de fato aconteça (Pinto, 2024).

Nesse sentido, o direito à construção da personalidade representa não apenas a proteção contra ingerências externas, mas também a promoção de condições que permitam ao indivíduo realizar-se enquanto ser humano, em consonância com seus próprios ideais e aspirações, tanto no âmbito individual, quanto social, nas palavras de Martins:

À medida que o ambiente em que se dá a vivência pessoal é alterado pelo próprio exercício da personalidade, novas possibilidades de exercício da autonomia surgem, bem como novas formas de subjugar essas práticas. Assim, os direitos da personalidade também devem ter permeabilidade às mudanças culturais e tecnológicas da realidade para que se possibilite o livre desenvolvimento da personalidade (Martins, 2021, p. 25).

Significa dizer que em condições ideais, o desenvolvimento da personalidade deve ser participativo e não sofrer opressões externas que se utilizem de força desproporcional sob os indivíduos, do contrário tal ambiente não será propício para que a personalidade se desenvolva de forma livre.

Em um dado momento histórico, o direito de personalidade foi entendido como um direito à liberdade negativa, relacionado ao não agir por parte do estado. As ameaças gravitavam em torno de questões como a vigilância estatal e controle político dos indivíduos. A figura de um ente com capacidade de opressão que pudesse interferir na liberdade e

consequentemente no desenvolvimento da personalidade era representada pela administração pública, aos moldes de uma figura Orwelliana, como na obra ficcional *1964* de George Orwell³¹ (Bauman; Lyon, 2014, p. 12).

Com o avanço tecnológico, as entidades privadas passaram a reconhecer o valor das informações e a utilizá-las para aprimorar produtos e estratégias de vendas. Os dados dos usuários tornaram-se objeto de interesse tanto de órgãos públicos quanto privados, por razões e objetivos diferentes.

Os interesses das entidades privadas em coletar e utilizar informações dos usuários estão diretamente ligados à otimização de seus negócios e à obtenção de vantagem competitiva ao conseguir inferir um comportamento de consumo e consequentemente prever determinados hábitos deste consumidor analisado. A problemática surge quando as informações dos usuários passam a ser acumuladas em excesso, sem uma finalidade específica.

À luz da teoria da identidade narrativa de Paul Ricoeur, a construção da identidade pessoal se dá por meio de uma articulação contínua entre a narrativa que o indivíduo constrói sobre si mesmo e aquela que é atribuída por outros, em um processo dialógico. A identidade, portanto, será o resultado do equilíbrio entre essas narrativas (Ricoeur, 1991).

Tradicionalmente a narrativa identitária se dá nos espaços de convivência e interação social, onde o indivíduo articula sua história a partir do diálogo e da convivência em contextos culturais como por exemplo, a família, a escola, os círculos de amizade, ambientes de trabalho e até mesmo os encontros fortuitos em espaços públicos são cenários em que a identidade se constrói.

Nos moldes tradicionais o insumo da narrativa, qual seja, a informação, é obtida com base naquilo que é informado por indivíduo e interlocutor, variáveis de acordo com o contexto. Note, portanto, que não há um mediador deste diálogo, e há uma oportunidade de contestação das informações, ao passo que o indivíduo tem a prerrogativa de escolha do que pretende ou não revelar sobre si e sobre o outro. A título de exemplo, é razoável afirmar que um indivíduo quando em seu ambiente de trabalho irá se comportar diferente de quando está

³¹1984 é um romance distópico escrito por George Orwell e publicado em 1949. A obra retrata uma sociedade totalitária e hipercontrolada, onde o Estado vigia todos os aspectos da vida dos cidadãos por meio de tecnologia e repressão, simbolizada pela figura onipresente do “Grande Irmão”. O livro é uma crítica à opressão política, à manipulação da verdade e à supressão das liberdades individuais, sendo considerado um dos mais influentes do século XX.

com seus amigos, aos moldes do que Altman chama *openness and closeness*³² de que pode ser entendido como gerenciamento do desejo daquilo que se quer ou não mostrar em determinado contexto (Altman. 1975).

Aqui a pesquisa avança no estado da técnica ao analisar que diferentemente de uma identidade narrativa tradicional, aqui compreendida como um direito de personalidade, a construção desta mesma narrativa soma-se a uma terceira figura, o algoritmo, que altura como um terceiro ator, responsável por registrar e organizar as informações. Entretanto não há para este uma imposição de limites de quais informações o devem ou não ser consideradas para a construção daquela identidade.

Entendemos por tanto que a narrativa do algoritmo é desproporcional frente ao usuário, devido à capacidade de acúmulo de informações, o que para os seres humanos seria a memória, para os algoritmos são uma base de dados com possibilidades infinitas de inferências traçadas quase que em tempo real, muitas vezes sem uma finalidade específica.

A narrativa passa a ser mediada, as interações do usuário (curtidas, compartilhamentos, buscas) alimentam sistemas e a partir destes registros geram perfis comportamentais a partir de um salvamento de informações inalcançáveis se comparada à um cérebro humano. Esses perfis, porém, não são meros espelhos da subjetividade, mas narrativas externas construídas a partir de lógicas comerciais, em que o grau de importância de cada preferência e/ou fato relativo ao indivíduo se dará de acordo como o perfil consumidor onde este melhor se enquadrar.

Bioni (2019) aborda a questão dos dados pessoais sob uma perspectiva de bens da personalidade, pois são uma projeção da pessoa humana. Todavia, entende que este novo direito se desdobra ao ponto de se tornar autônomo, pois forma um novo tipo de identidade, e como consequência o titular teria a prerrogativa de retificação desses dados para que sua projeção seja precisa, (Bioni, 2019, p. 65).

Quando um algoritmo classifica um usuário como "propenso a compras impulsivas" ou "interessado em conteúdos políticos de esquerda", ele impõe uma interpretação reducionista que pode colidir com a autoimagem reflexiva do sujeito já que não há uma racionalidade e/ou um juízo de valor de quais características o indivíduo/consumidor gostaria que prevalecesse.

³² Controle da “abertura” ou “fechamento”, imposição de limites, para acesso a algo que é considerado privado pelo indivíduo, por exemplo, informações pessoais.

Esta perfilização interfere nesse processo ao sobrepor uma narrativa externa, elaborada a partir de dados automatizados, à narrativa interna do sujeito, dificultando sua apropriação reflexiva e autônoma da própria história. Dessa forma, a interferência algorítmica pode restringir a liberdade do indivíduo de construir e reconstruir sua identidade narrativa, comprometendo a privacidade necessária para a autorreflexão e consequentemente um desenvolvimento da personalidade de maneira livre.

Por óbvio, um excesso de privacidade em que nenhuma informação pudesse ser mostrada seria contrário a própria natureza de uma rede social, onde se propõe uma interação e trocas de informações, todavia o que se pontua aqui é a possibilidade de uma ponderação de interesses.

Em síntese, apenas em um contexto em que as narrativas forem justas será possível o desenvolvimento saudável da personalidade e partir destas narrativas será possível ao usuário desenvolver sua identidade, entendendo esta como um dos aspectos necessários à personalidade. Os conceitos de identidade e sua forma de desenvolvimento serão analisados no próximo item.

3.4 Redes sociais, *profiling* e identidade

3.4.1 *Profiling* como fato social

O conceito de “norma” é central para Durkheim na classificação dos fatos sociais porque, para ele, fatos sociais são justamente as regras, padrões e expectativas coletivas que orientam e regulam o comportamento dos indivíduos em uma sociedade. Durkheim afirma que fatos sociais são maneiras de agir, pensar e sentir que são exteriores ao indivíduo e dotadas de um poder de coerção pelo qual se impõem a ele. Ou seja, são normas sociais que existem independentemente das vontades individuais e exercem pressão para que os indivíduos as sigam (Durkheim, 1999).

Assim, a presença de uma norma, entendida como um padrão coletivo de conduta, pensamento ou sentimento, é o que permite identificar um fato social. A norma social manifesta-se, por exemplo, nas regras de comportamento nas redes sociais, nos padrões de consumo, nas expectativas de privacidade, entre outros. Quando um comportamento se torna generalizado, exterior ao indivíduo e coercitivo, ele adquire o status de norma e, portanto, de fato social, segundo a teoria desenvolvida pelo sociólogo Émile Durkheim: “*Fatos sociais*

são maneiras de agir, de pensar e de sentir, exteriores ao indivíduo, e que são dotadas de um poder de coerção em virtude do qual se impõem a ele” (Durkheim, 2007, p. 13-14).

De acordo com Durkheim, para identificar um fato social na análise de comportamentos coletivos, segundo Durkheim, é preciso observar se o fenômeno apresenta três características essenciais:

- **Exterioridade**: O comportamento, regra ou prática existe fora do indivíduo, ou seja, é imposto pela sociedade e não depende da vontade pessoal. Por exemplo, as normas de uso das redes sociais ou a cultura do consentimento digital não são criadas individualmente, mas são estabelecidas coletivamente e os indivíduos apenas as seguem.
- **Coercitividade**: O fato social exerce uma pressão sobre os indivíduos, obrigando-os a agir de determinada maneira sob pena de sanções (explícitas ou implícitas). No contexto das redes sociais, quem não adere a certos padrões de comportamento pode sofrer exclusão, críticas ou perder oportunidades, demonstrando o caráter coercitivo do fenômeno.
- **Generalidade**: O fato social é comum a muitos membros da sociedade, manifestando-se de forma regular e recorrente. Por exemplo, a prática do profiling e o aceite dos termos de uso são comportamentos adotados por milhões de usuários, tornando-se padrão coletivo.

3.4.2 *Profiling* e identidade

Diante da multiplicidade de contextos que contribuem para a construção da personalidade de um indivíduo, como contexto familiar, socioeconômico, cultural, escolar, entre outros, esta pesquisa se propõe a analisar o desenvolvimento da personalidade no contexto das redes sociais, utilizando como ponto de partida neste item, a teoria behaviorista e a identidade narrativa, a fim de desmontar como a padronização identitária pode influenciar a formação da identidade no contexto das redes sociais (Skinner, 1953).

Ao rotular sujeitos com base em correlações probabilísticas, tais sistemas contribuem para uma forma de identidade construída por terceiros, que independe da narrativa subjetiva de quem é perfilado. Com isso, emerge uma forma de padronização da identidade, que não considera a complexidade da experiência humana e suas possibilidades de mudança e reinvenção (Ricoeur, 1991).

Um exemplo emblemático disso é o sistema de recomendação do Facebook, que sugere conteúdo com base em interações anteriores, reforçando traços comportamentais observados e dificultando a exposição a perspectivas divergentes³³ (Bakshy; Messing; Adamic, 2015)

No item anterior foi abordada a importância da privacidade no livre desenvolvimento e disparidade de informações entre os interlocutores, a função dos algoritmos na construção da narrativa e a força desproporcional entre as partes diante da capacidade máquina x homem de acumular informações sobre o outro.

A teoria behaviorista, especialmente em sua vertente radical proposta por B. F. Skinner (1953), fundamenta-se na ideia de que o comportamento humano pode ser compreendido como resposta observável a estímulos externos, dispensando a consideração de estados internos, intencionalidade ou consciência. Essa lógica de previsibilidade e controle do comportamento, baseada exclusivamente em observações empíricas e mensuração de respostas, constitui o ponto de partida para interpretações contemporâneas do comportamento em ambientes digitais.

Antoinette Rouvroy (2013) avança essa perspectiva ao propor o conceito de “behaviorismo de dados”, que descreve a forma como os sistemas algorítmicos atuais produzem conhecimento e intervenção comportamental a partir de padrões extraídos de grandes volumes de dados. Ao contrário das abordagens psicológicas tradicionais, essa nova forma de comportamento mediado por dados prescinde completamente da compreensão subjetiva dos indivíduos. Para a autora:

A crença implícita que acompanha o crescimento do ‘Big Data’ é que, desde que se tenha acesso a enormes quantidades de dados brutos [...] é possível antecipar a maioria dos fenômenos (incluindo os comportamentos humanos) do mundo físico e do mundo digital, graças a algoritmos relativamente simples que permitem, numa base estatística puramente indutiva, construir modelos de comportamentos ou padrões, sem ter que considerar causas ou intenções. Chamarei de ‘behaviorismo de dados’ essa nova maneira de produzir conhecimentos sobre atitudes preferenciais futuras, comportamentos ou eventos sem considerar as motivações psicológicas, os discursos ou as narrativas do sujeito, mas sim com base em dados.” (Rouvroy, 2013, p. 2).

³³ Conforme investigado por Bakshy et al. (2015), o algoritmo do Facebook tende a filtrar conteúdos politicamente diversos, reforçando preferências já existentes dos usuários.

Esse modelo de análise automatizada, descolado da interioridade do sujeito, evidencia como os sistemas de perfilamento contemporâneos reproduzem uma lógica puramente reativa: classificam, preveem e intervêm a partir de estímulos anteriores observáveis, apagando a subjetividade e desvalorizando a narrativa pessoal. Ao lado de Rovroy, Shoshana Zuboff também denuncia a ascensão de um sistema técnico-econômico orientado pela captura e modulação de comportamentos futuros, baseado em reforços digitais semelhantes ao modelo behaviorista radical (Zuboff, 2020).

Observa-se então uma aproximação conceitual entre a lógica do behaviorismo de dados e o conceito de mesmidade (idem) em Paul Ricoeur, onde o sujeito perfilado por sistemas algorítmicos é reduzido à repetição de traços anteriores, à constância estatística, ou seja, à sua identidade objetiva e previsível. Comprometendo a construção narrativa da identidade, a ipseidade, que envolve escolha, mudança e responsabilidade é suprimida por um modelo que classifica e antecipa ações com base apenas no comportamento passado (Ricoeur, 1991).

Assim, a lógica algorítmica compromete a capacidade do indivíduo de narrar a si mesmo e de modificar sua trajetória, comprometendo o livre desenvolvimento da personalidade. Essa tensão entre mesmidade e ipseidade está no cerne dos impactos identitários provocados pela prática de perfilamento digital (Ricoeur, 1991).

Neste item daremos ênfase aos usuários, adentraremos nos reflexos da perfilização na identidade, para demonstrar de que forma perfilização pode interferir na capacidade de uma narrativa coerente dos indivíduos no contexto das redes sociais., comprometendo a construção da identidade ao desequilibrar as dimensões de *mesmidade* e *ipseidade*, utilizando para tanto referencial teórico de Paul Ricoeur estudado na obra *O Si mesmo como um outro* (Ricoeur, 1991).

Para Ricoeur (1991), a identidade pessoal é constituída por meio da articulação de experiências em narrativas, permitindo ao indivíduo atribuir sentido à própria existência ao integrar passado, presente e futuro em um processo compartilhado, no qual o sujeito é tanto autor quanto leitor de sua própria vida. A identidade narrativa se constrói na intersecção entre a história que o indivíduo conta sobre si mesmo e a história que outros contam sobre ele, sendo fundamental para a afirmação e reconhecimento da individualidade.

O autor considera o ato de narrar como a capacidade de explicar a si mesmo, organizando eventos em uma trama que vai além da mera sucessão cronológica, mas dos fatos que dentro destes acontecimentos são entendidos pelo indivíduo para a sua auto narração e

construção da identidade através de dois elementos principais, a mesmidade *Iden* e a Ipseidade *Ipse* (Ricoeur, 1991).

Dentro desta lógica a mesmidade refere-se à permanência, à identidade como continuidade e semelhança consigo mesmo ao longo do tempo, englobando características objetivas e estáveis do sujeito. Já a ipseidade designa a identidade reflexiva, dinâmica e responsável, que permite ao indivíduo manter-se fiel a si mesmo diante das mudanças, assumindo compromissos e promessas. Essa dialética é especialmente relevante no registro da narração, pois é na identidade narrativa que mesmidade e ipseidade se articulam, permitindo ao sujeito apropriar-se de sua história de forma reflexiva (Ricoeur, 1991).

Para Ricoeur (1991), a narrativa não é apenas um ato solitário do indivíduo, mas um processo mediado e compartilhado. O sujeito é considerado tanto leitor quanto autor de sua própria vida, pois a identidade narrativa se constrói na intersecção entre a história que ele conta sobre si mesmo e a história que outros contam sobre ele. Isso implica que a identidade pessoal é sempre parcialmente opaca ao próprio sujeito, que só se reapropria de si mesmo por meio dos sinais, obras e monumentos que resultam de sua atividade e interação social. A narrativa, portanto, é uma tarefa coletiva e dialógica, ainda que o protagonismo da autoria recaia sobre o indivíduo.

Nesse contexto, as plataformas digitais, especialmente o Facebook e o Instagram da Meta Platforms Inc., desempenham papel ativo na mediação de experiências e relações humanas, das quais não se pode mais rejeitar a influência, conforme observado no diálogo de Bauman e Lyon:

A sociologia agora é obrigada a se entender com o digital para não deixar de investigar e teorizar sobre espaços inteiros de atividade cultural significativa. Para início de conversa, a simples dependência tecnológica tem de ser considerada relevante em qualquer explicação social digna desse nome. São tantos os relacionamentos em parte – ou na totalidade – vivenciados on-line que uma sociologia sem o Facebook é inadequada. Independentemente de como o entenda a geração mais velha, o Facebook se tornou um meio básico de comunicação – de “conexão”, como expressa o próprio Facebook – e é agora uma nova dimensão da vida cotidiana para milhões de pessoas. (Bauman; Lyon, 2014 p. 32).

Como pontuado pelos autores, o Facebook e o Instagram, figuram como este novo espaço de atividade cultural, porém com características próprias e parâmetros distintos, como uma nova versão de sociedade onde os usuários são incentivados a compartilhar fragmentos de suas vidas, selecionando quais aspectos desejam tornar públicos e quais preferem manter

em privado (Bowden-Green et al., 2021). Essa dinâmica transforma as redes sociais em arenas de construção e disputa de narrativas, onde a identidade é constantemente negociada e performada.

A necessidade de validação social, reforçada por mecanismos como curtidas, comentários e compartilhamentos, intensifica a pressão para que o usuário adote comportamentos alinhados às expectativas do grupo (Skinner, 1953). O algoritmo, ao priorizar conteúdos que maximizam engajamento, restringe a exposição a perspectivas divergentes, limitando o contato com narrativas alternativas e reforçando padrões de conformidade (Bowden-Green et al., 2021).

Essa dinâmica coloca em risco a autenticidade e a coerência da narrativa pessoal, pois a competição de narrativas acontece de forma injusta, as redes sociais criam perfis sobre os indivíduos dos quais eles mesmos podem não saber de forma consciente, ou contestar esta narrativa, sendo induzidos a querer gostar e acreditar naquele conteúdo ao qual estão constantemente sendo submetidos, já que os algoritmos tendem a incentivar a conformidade e a padronização de comportamentos, o que compromete o livre desenvolvimento da personalidade e a autodeterminação informativa, direitos assegurados pela LGPD e fundamentais para a dignidade humana.

Algoritmos de *profiling* categorizam usuários com base em padrões comportamentais, restringindo a exposição a conteúdos diversificados e incentivando conformidade, de forma que os usuários são instigados a mostrar os fragmentos de sua personalidade que são aceitos naquele contexto, assim o indivíduo é incentivado a construir uma personalidade para aquele contexto, não com base na sua percepção de si, mas com base na versão que tende a ser validada pelos pares.

Partindo da premissa de que o insumo para a construção de narrativas é a informação sobre si, que, após assimilada pelo indivíduo, é organizada em uma história de vida, o resultado desse processo é a constituição da identidade narrativa. Segundo Paul Ricoeur, essa identidade se forma de maneira intersubjetiva, na articulação entre a narrativa que o indivíduo constrói sobre si e aquela que é atribuída pelo contexto social em que está inserido.

Aqui neste trabalho considera-se a internet como um desses contextos em que se forma a identidade, um novo contexto característico da sociedade contemporânea, em que o usuário novamente irá narrar e ser narrado, porém aqui neste trabalho se discute o fato de uma destas narrativas, no caso a da rede social, ocorrer com um número muito maior de informações.

Enquanto os indivíduos escolhem os aspectos de sua vida que consideram marcantes e relevantes para diferenciar um *eu* do *outro* priorizando algumas informações em detrimento de outras, e até mesmo descartando alguns comportamentos já que não é humanamente possível de se registrar tudo o que se faz a todo o tempo, as redes sociais através dos sistemas de *big data*, conseguem registrar e armazenar toda a atividade do usuário na plataforma, registrando mais informações sobre o usuário do que ele mesmo guarda de si, e com base nestas informações construir a narrativa sobre a pessoa.

Sobre a afirmação feita no parágrafo anterior podemos trazer a pesquisa realizada Cambridge e Stanford, que analisaram a capacidade de se extrair traços da personalidade de uma pessoa através das curtidas de conteúdos no Facebook para aferir sobre 5 grandes traços de personalidade, sendo eles abertura, conscienciosidade, extroversão, amabilidade e neuroticismo. Como amostra, foram escolhidos 86.220 voluntários que foram submetidos aos conteúdos enquanto seus amigos e familiares avaliavam estes indivíduos com base em sua personalidade, e a partir daí criarem uma comparação das respostas (Ghosh, 2015).

Os resultados indicaram que com apenas 10 curtidas o algoritmo conseguia prever a personalidade de um usuário melhor que um colega de trabalho, melhor que um amigo com 70 curtidas, melhor que um familiar com 150 curtidas e com 300 curtidas o algoritmo saberia mais da personalidade do usuário do que seu próprio cônjuge (Kosinski; Stillwell; Graepel, 2013).

Tal informação demonstra que a captação das atividades dos usuários pode ter implicações na própria subjetividade, pois os conteúdos aos quais terá acesso serão auferidos a partir deste perfil, formando uma bolha, ou como abordado por Sérgio Amadeu da Silveira, guetos ideológicos, que impossibilita o contato com informações diferentes, ocasionais e fortuitas, tangenciando o próprio rumo da vida (Bioni, 2019; Silveira, 2017, p. 88).

A pesquisa buscou entender quantas curtidas em média um cidadão brasileiro efetua em um determinado tempo espaço, mas tal informação não foi encontrada, tampouco foram localizados estudos acadêmicos revisados por pares que investigassem especificamente o número de curtidas do usuário nas redes sociais da empresa meta. Entretanto, foi localizada uma pesquisa do site *Brandwatch*, uma plataforma de monitoramento e análise de mídia social, datado de 2018, que apontava que um usuário deixava em média 10 curtidas por mês, média de 120 curtidas por ano, com um tempo médio de 20 minutos por dia no site, (Smith, 2019). Contudo, se reconhece a limitações metodológicas e a necessidade de cautela na interpretação dos números indicados pela fonte.

Vale ressaltar aqui alguns pontos importantes, o primeiro sobre a data da pesquisa, 2018, de modo que tais números podem estar defasados, já que a própria pesquisa informa que o Facebook adicionava à época 500.000 novos usuários por dia, 6 novos perfis a cada segundo (Smith, 2019).

Outro ponto relevante é que a pesquisa não indica a origem dos usuários utilizados na amostragem, aparentando ser uma média global dos usuários, todavia, tempo de 20 minutos é bem abaixo do tempo gasto pelos usuários brasileiros que de acordo com pesquisas recentes é o terceiro maior público consumidor de redes sociais no mundo.

Outra variação importante é em relação à idade, visto que de acordo com pesquisas recentes que foram indicadas neste trabalho, adolescentes podem passar mais de três horas por dia conectados na rede social, logo pode-se concluir que o número de curtidas de um usuário brasileiro em 2025 tende a superar o número de 10 curtidas por mês, bem como a média de 20 minutos de uso diário. Reconhece-se a possibilidade de distanciamento desses dados em relação ao contexto brasileiro. Ainda assim, optou-se por mantê-los na pesquisa, compreendendo que, na ausência de outras fontes, tais dados podem fornecer um parâmetro mínimo de comparação para a análise desenvolvida.

Importante trazer ao trabalho que os impactos da rede social no comportamento humano ainda é um campo cujo conhecimento se encontra em estágio incipiente. Parte deste desconhecimento é devido à coexistência de três gerações com experiências tecnológicas distintas: idosos (formados previamente à informatização), adultos (transição analógico-digital) e jovens (nativos digitais). Essa heterogeneidade dificulta a generalização de efeitos, pois cada grupo internaliza a tecnologia de forma única, com valores e hábitos moldados por diferentes contextos históricos.

Entretanto, estudos apontam que o uso intensivo dessas plataformas está associado ao aumento de transtornos como ansiedade, depressão e distúrbios alimentares, além de contribuir para a polarização social e a deterioração da autoimagem. Tais impactos são potencializados por algoritmos que promovem conteúdos altamente engajadores e reforçam padrões de comportamento, o que suscita discussões relevantes sobre autodeterminação informativa e livre desenvolvimento da personalidade nestes ambientes (Machado, 2024).

No mesmo sentido, pesquisa realizada pela Universidade de Oxford em 2024 revelou que adolescentes que passam mais de três horas por dia nas redes têm 60% mais chances de desenvolver depressão. A investigação aponta o impacto da cultura digital na reconfiguração

da formação emocional e psicológica e a necessidade de regulação específica de redes sociais (Pacete, 2025).

Um exemplo paradigmático da interferência dos sistemas de perfilamento na construção da identidade dos indivíduos pode ser observado no caso do algoritmo COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*), amplamente utilizado no sistema de justiça criminal dos Estados Unidos. Esse sistema computacional era empregado para estimar o risco de reincidência de réus, influenciando decisões judiciais sobre fiança, sentenças e liberdade condicional (Angwin *et al.*, 2016).

Em 2016, uma investigação do veículo ProPublica, organização de jornalismo investigativo, demonstrou que o algoritmo apresentava vieses raciais significativos: réus negros eram erroneamente classificados como de alto risco de reincidência quase duas vezes mais do que réus brancos, mesmo sem diferenças relevantes nos históricos criminais (Angwin *et al.*, 2016).

Embora se trate de um sistema utilizado no contexto judicial, o caso COMPAS fornece uma análise empírica valiosa sobre os efeitos identitários do perfilamento algorítmico. Ao atribuir uma identidade de risco com base em padrões estatísticos opacos e enviesados, o algoritmo influenciava a percepção institucional e social do réu, interferindo diretamente em sua narrativa pessoal e em sua autonomia.

Essa dinâmica ilustra como sistemas automatizados podem capturar e redefinir trajetórias individuais a partir de dados anteriores, muitas vezes sem possibilidade de contestação ou revisão. Tais impactos, como discutido ao longo deste item, comprometem o livre desenvolvimento da personalidade, especialmente quando ocorrem em contextos marcados por assimetria técnica e ausência de transparência, características também presentes nas redes sociais digitais investigadas neste trabalho.

Dessa forma, evidencia-se que a prática do *profiling* não apenas representa uma técnica de segmentação mercadológica, mas também um mecanismo de poder simbólico e informacional que compromete, estruturalmente, os direitos à identidade e à autodeterminação informativa no ambiente digital contemporâneo.

3.5 A narrativa líquida: uma intersecção entre os conceitos de *modernidade líquida* de Zygmunt Bauman e a *identidade narrativa* de Paul Ricoeur aplicados ao *profiling*

A intersecção entre a *modernidade líquida* de Zygmunt Bauman e a *identidade narrativa* de Paul Ricoeur oferece um arcabouço teórico fértil para analisar os impactos do *profiling* algorítmico nas redes sociais. Enquanto Bauman descreve um mundo marcado pela fluidez, insegurança e vigilância difusa, Ricoeur propõe que a identidade se constrói na dialética entre permanência (*idem*) e transformação (*ipse*), mediada por narrativas. Este trabalho articula esses conceitos para entender como a coleta massiva de dados e a modulação comportamental interferem na autonomia narrativa dos usuários, transformando-os em objetos de decisões automatizadas.

Bauman (2018) define a *modernidade líquida* como uma era de dissolução de estruturas sólidas — como instituições, relações e identidades —, substituídas por dinâmicas flexíveis, efêmeras e individualizadas. Nesse contexto, a vigilância deixa de ser um mecanismo centralizado e opressivo (como no panóptico de Foucault) para se tornar *líquida*: invisível, adaptável e internalizada pelos indivíduos como parte da experiência cotidiana (Bauman; Lyon, 2018). Nas redes sociais, essa vigilância se materializa no *profiling*, técnica que coleta dados comportamentais para criar perfis preditivos, os quais orientam desde publicidade personalizada até a curadoria de conteúdo.

A lógica do *capitalismo de vigilância* (Zuboff, 2020), não citada, mas implícita na análise de Bauman, evidencia que os dados dos usuários são comoditizados, transformando subjetividades em insumos para modelos de negócios. A fluidez da vigilância líquida reside na capacidade dos algoritmos de se remodelarem continuamente, antecipando desejos e normalizando a exposição constante, o que corrói a noção de privacidade e autonomia.

O que se propõe neste item é um paralelo entre a mesmidade da teoria narrativa com o que Bauman entenderia como sólido, enquanto a ipseidade de Ricoeur, aquilo que é volátil e dinâmico guardaria uma relação com a liquidez amplamente abordada por Bauman, aqui analisada como uma resposta a liquefação da identidade identitária, que seria resultado da instabilidade narrativa das redes sociais. A própria identidade passa a ter que se adaptar à dinâmica das redes sociais.

O paradoxo então consiste na capacidade do indivíduo de se manter fiel a si mesmo ao passo que também precisa se adaptar ao contexto social, manter se em uma narrativa coerente em um contexto fragmentado e narrado por um algoritmo que atualiza os perfis em tempo

real, tornando a identidade um fluxo de dados maleável, sem centro fixo (Bauman; Lyon, 2018, p. 47).

Ao passo que a ipseidade da narrativa necessita de transparência para que o indivíduo possa raciocinar sobre os fatos, de maneira crítica, uma autoavaliação e seleção dos fatos que este considerar relevantes enquanto a opacidade da narrativa algorítmica é o extremo oposto de transparência, logo não seria possível ao indivíduo dialogar com esta terceira identidade, já que não se sabe qual o caminho feito até que se chegasse aquela construção.

A *identidade narrativa* surge da articulação entre essas dimensões, permitindo ao sujeito integrar experiências passadas, presentes e expectativas em uma história coerente. Nas redes sociais, entretanto, o *profiling* cristaliza o *idem* ao reduzir o usuário a padrões comportamentais quantificáveis (ex: “consumidor de moda sustentável”), enquanto limita o *ipse* ao restringir o acesso a conteúdo dissonantes (bolhas algorítmicas). A narrativa externa, construída por algoritmos, sobrepõe-se à auto interpretação, fragilizando a mediação reflexiva essencial à identidade (Ricoeur, 1991, p. 169).

Por exemplo, ao priorizar conteúdos alinhados a preferências passadas (*idem*), as redes sociais restringem a exposição a perspectivas que desafiem o *status quo* (ex: notícias divergentes, diversidade de corpos, raça e perfiz de beleza), limitando a capacidade de ressignificação (*ipse*) e convivência com o diverso. Essa dinâmica reforça a *passividade líquida* descrita por Bauman, na qual os indivíduos são “consumidores de identidades” em vez de autores de suas histórias.

A ideia de que a repetição de uma imagem, ideia ou estímulo aumenta sua aceitação ou familiaridade, mesmo sem compreensão racional ou argumentativa, não se faz algo novo, tampouco foi introduzida pelas redes sociais e foi observada há mais de seis décadas pelo psicólogo social Robert Zajonc (1968), em sua formulação do efeito da mera exposição. O efeito da mera exposição, formulado por Robert Zajonc em 1968, é uma teoria da psicologia social que demonstra que a simples repetição de um estímulo aumenta a probabilidade de que ele seja percebido de forma positiva ou familiar, mesmo sem que haja entendimento consciente ou análise crítica.

De forma complementar, a teoria da *Janela de Overton*, proposta por Joseph P. Overton, na década de 1990, sugere que existe uma faixa de ideias consideradas “aceitáveis” pela opinião pública em determinado momento, chamada de “janela”. Ideias fora dessa janela são vistas como radicais ou impensáveis. No entanto, com exposição gradual, reformulação de

linguagem e repetição estratégica, ideias inicialmente inaceitáveis podem migrar para o centro do debate público, tornando-se aceitáveis, populares e até políticas oficiais.

A título de exemplo, uma pesquisa psiquiátrica, realizada com adolescentes brasileiras do estado de São Paulo, abordou a influência das redes sociais com a insatisfação da imagem corporal. Segundo o estudo a imagem corporal pode ser definida a partir da internalização da ideia de “corpo ideal” ideal construída em nossa mente, e que tal internalização é capaz de modificar comportamentos pessoais. A pesquisa argumenta ainda que dos diversos fatores que influenciam a construção da autoimagem, três deles têm maior importância, sendo: Os pais, os amigos e a mídia, além de identificar um aumento de insatisfação corporal entre 6,57 e 4,47 vezes maior nas meninas que acessam os aplicativos Facebook e Instagram mais de 10 vezes diariamente (Lira, 2017; Rezende, 2020).

O que se explana neste item é a perfilização enquanto mediadora responsável por escolher o contexto onde cada indivíduo será exposto nas redes sociais, mediando o diálogo entre o interno e o externo, o si e o outro, expondo os usuários de forma reiterada aos interesses que dele foram inferidos, assumindo um papel narrativo nesta dinâmica capaz de influenciar a percepção do indivíduo, que tende a reagir como fruto do meio, tal qual exposto na teoria behaviorista, agora adaptada para o ambiente digital.

Essa dinâmica reforça a função narrativa do *profiling*, que não apenas organiza as experiências digitais dos sujeitos, mas também limita os sentidos possíveis a partir de padrões previamente inferidos. Nesse cenário, torna-se possível identificar efeitos mais amplos sobre a construção identitária, os quais podem ser aprofundados a partir do diálogo entre as teorias de Zygmunt Bauman e Paul Ricoeur.

O paralelo entre Bauman e Ricoeur evidencia que o *profiling* nas redes sociais opera uma dupla captura: liquefaz identidades ao reduzi-las a dados voláteis e congela narrativas ao impor lógicas preditivas.

Assim, ao colocar estes conceitos em diálogo, observa-se que o fenômeno do *profiling* algorítmico nas redes sociais promove uma dupla distorção na identidade do sujeito contemporâneo: por um lado, reduz o sujeito à mesmidade (idem), cristalizando padrões comportamentais previsíveis; por outro, esvazia sua ipseidade, impedindo a reconstrução reflexiva da própria narrativa.

Diferentemente da identidade narrativa proposta por Ricoeur, cujo foco reside no processo contínuo de interpretação de si ao longo do tempo, a narrativa construída pelas redes sociais possui um caráter marcadamente finalístico. Trata-se de uma construção orientada à

finalidade de classificação e monetização, em que a formação do perfil do usuário visa à estabilização de categorias de consumo. Essa identidade algorítmica é operada não em função da subjetividade do sujeito, mas em prol dos interesses de terceiros, anunciantes, plataformas e sistemas de recomendação

Nesse processo, a identidade deixa de ser um projeto contínuo de si e passa a ser moldada por fluxos externos, invisíveis e instáveis, e em velocidades incompatíveis com a reflexão e maturação dos fatos percebidos, coerente com a lógica da modernidade líquida.

Ao contrário da construção identitária tradicional, em que a ipseidade se desenvolve por uma narrativa contínua, reflexiva, aberta e sem almejar um fim em si mesmo, na narrativa algorítmica a construção assume um caráter finalístico, moldando-se conforme interesses de mercado. Nela, não se considera a subjetividade, mas apenas a previsibilidade de respostas a estímulos externos específicos, com base em padrões de comportamento.

Essa dinâmica resulta em uma narrativa instável e fluida, marcada pela ausência de centro fixo e pela oscilação constante, características que se aproximam da liquidez descrita por Zygmunt Bauman. Por essa razão, ao interseccionar as teorias da identidade narrativa e da modernidade líquida e aplicá-las ao objeto deste trabalho, propõe-se a noção de “narrativa líquida” como a expressão da subjetividade mediada por algoritmos.

4 A ERA DA INFORMAÇÃO – ECONOMIA DE VIGILANCIA, DATIFICAÇÃO DA VIDA E SEUS IMPACTOS NO COMPORTAMENTO HUMANO

Esta seção visa trazer a pesquisa esclarecimentos técnico e semânticos sobre decisões automatizadas, na qual se inclui a perfilização/*Profiling*, aqui tratados como sinônimos, trazendo os conceitos e classificações do instituto necessárias ao entendimento da pesquisa. Considerando a insuficiência de conceitos jurídicos na legislação brasileira, tomaremos emprestados alguns conceitos e comandos da lei geral de proteção de dados alemã, General Data Protection (GDPR), instituto no qual se inspirou a Lei de Proteção de Dados Brasileira.

4.1 O que é *Profiling*? Classificação no Tratamento Automatizado de Dados

Por meio de métodos algorítmicos, grandes volumes de informações sobre usuários são coletados, analisados e utilizados para a construção de perfis, que normalmente visam estabelecer um padrão específico em um contexto específico, por exemplo análise de score para linha de crédito, análise de perfil profissional para fins de admissão de candidatos em uma vaga de emprego.

Ocorre que nas redes sociais, a construção de perfis não segue uma lógica específica, todos os dados são igualmente considerados e mapeados a após a identificação do comportamento é que se direciona os conteúdos e ou produtos de interesse, observe, portanto, que não há uma finalidade definida ao tempo da captura desses dados, e desta ausência de finalidade surgem as discussões sobre os limites e impactos dessa prática nos direitos fundamentais.

A lei traz uma seção específica só para a definição de institutos, no artigo 4º, classificando separadamente o que é o tratamento de dados e suas subdivisões (onde inclui meios automatizados ou não automatizados), logo, o tratamento de dados é gênero do qual a perfilização é espécie. e o que é uma definição de perfiz, classificando esta como esta, uma forma de tratamento, Art. 4º:

«Tratamento», uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a

recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição; (União Europeia, 2016).

Do ponto de vista técnico, a A GDPR define *profiling* (ou perfilização) como: qualquer forma de tratamento automatizado de dados pessoais que visa avaliar aspectos pessoais de um indivíduo, prevendo comportamentos, preferências, interesses, desempenho profissional, situação econômica, saúde, localização, entre outros. Vide:

«Definição de perfis», qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspectos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspectos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações (UE) 2016/679, art. 4º. 4;

No contexto jurídico brasileiro, a LGPD não traz uma definição expressa de *profiling*, mas faz referência indireta ao tema em dispositivos como o art. 12, §2º e o art. 20. Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade

É importante distinguir as diferentes espécies de dados que são utilizados em um processo de perfilização, pois como definido pela própria LGPD, apenas dados pessoais estão sob o escopo da lei :

- (i) **Dados pessoais:** informações relacionadas a pessoa natural identificada ou identificável (LGPD, art. 5º, I).
- (ii) **Dados inferidos:** informações deduzidas a partir do cruzamento de dados triviais, muitas vezes não fornecidas diretamente pelo titular, mas inferidas por algoritmos (Kosinski, Stillwell & Graepel, 2013).

(iii) **Dados anonimizados:** aqueles que, isoladamente ou em conjunto, não permitem a identificação do titular, exceto se o processo de anonimização puder ser revertido (LGPD, art. 5º, III; art. 12).

A distinção é relevante porque o *profiling* frequentemente utiliza dados inferidos e anonimizados para criar perfis, que em tese não são abarcados pelas regras da LGPD, visto que a legislação foi silente neste ponto, como consequência, restam dúvidas razoáveis nas discussões doutrinárias sobre o alcance da Lei de Proteção de dados brasileira sobre o tratamento de dados inferidos e anonimizados que não são capazes de revelar a identidade do usuário, mas igualmente conseguem afetar o contexto em que o usuário está inserido nas redes sociais.

Por outro lado, o regulamento alemão aborda a perfilização de forma mais detalhada, tratando-a como uma categoria específica de tratamento de dados pessoais. Por essa razão, ela é submetida a regras próprias e salvaguardas adicionais, especialmente nos casos em que decisões são tomadas de forma automatizada, sem qualquer intervenção humana ou com intervenção humana apenas residual. Essa disciplina está prevista no artigo 22 do referido regulamento.:

Art. 22. Decisões individuais automatizadas, incluindo definição de perfis
O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.

Entretanto, tal qual a LGPD, a GDPR também limita seu escopo de atuação aos tratamentos de dados pessoais, ficando silente quanto à perfilização feita a partir de dados não pessoais obtidos através de inferências, como é o caso dos dados tratados pelas plataformas da Meta. Da leitura da legislação pode se concluir que a perfilização foi pensada para os casos de tomadas de decisões específicas sobre os usuários, não conseguindo alcançar os tratamentos de dados para fins genéricos.

A lacuna normativa se torna mais evidente diante do uso de dados, não pessoais, dados inferidos (aqui incluídos os não pessoais, pessoais e sensíveis) e dados coletivos. No contexto da perfilização, é fundamental distinguir entre os direitos subjetivos, que afetam indivíduos identificáveis, e os direitos supraindividuais, cujos efeitos incidem sobre grupos inteiros ou coletividades. Neste último caso, os impactos ocorrem de forma difusa, sem que seja possível

identificar com precisão um sujeito diretamente lesado, o que dificulta não apenas a caracterização do dano, mas também a demonstração do nexo de causalidade entre o fato e a lesão, comprometendo a responsabilização jurídica.

A problemática aumenta: além dos dados inferidos, acrescentam-se os dados coletivos, pois, em se tratando de perfilização, existem os direitos subjetivos e os direitos supraindividuais, que afetam uma coletividade sem que seja possível uma individualização do dano.

Como resultado, eventual ou potencial dano causado aos direitos fundamentais de usuários ou grupo de usuários necessitaria de uma comprovação, com respaldo na combinação de diversos institutos jurídicos, como os direitos do consumidor, lei de proteção de dados, estatutos de criança adolescente e idoso, cada qual analisado de acordo com o caso concreto pelo judiciário.

Entretanto, essa ausência de comandos legislativos e administrativos reforça a assimetria de informação entre as partes, visto ser extremamente difícil para um cidadão médio conseguir comprovar um nexo de causalidade entre violações de direitos da personalidade e a prática de perfilização da empresa Meta. Platform Inc. o que, na prática, é benéfico para as redes sociais da empresa.

Diante desse cenário, a doutrina e órgãos como a ANPD têm apontado a necessidade de:

- **Interpretação hermenêutica ampliada:** Aplicação dos princípios constitucionais do livre desenvolvimento da personalidade e autodeterminação informativa para ampliar o escopo da proteção, incluindo dados inferidos e impactos coletivos.
- **Salvaguardas adicionais:** Implementação de medidas como transparência algorítmica, direito à explicação, avaliações de impacto algorítmico e participação ativa da autoridade reguladora (Bioni, 2019; Martins, 2021).
- **Relatórios de impacto:** Adoção de instrumentos como o Data Protection Impact Assessment (DPIA), previstos na LGPD (art. 38), para operações de *profiling*, promovendo abordagem preventiva e transparente

Diante desse cenário, a doutrina e órgãos como a ANPD têm apontado a necessidade de uma interpretação hermenêutica ampliada, com a aplicação dos princípios constitucionais do livre desenvolvimento da personalidade e da autodeterminação informativa para ampliar o

escopo da proteção, incluindo dados inferidos e impactos coletivos (Bioni, 2019; Martins, 2021).

Além disso, destaca-se a importância da implementação de salvaguardas adicionais, como a transparência algorítmica, o direito à explicação, avaliações de impacto algorítmico e a participação ativa da autoridade reguladora, conforme defendem Bioni (2019) e Martins (2021). Por fim, ressalta-se a adoção de instrumentos como o *Data Protection Impact Assessment* (DPIA), previstos na LGPD (art. 38), para operações de *profiling*, promovendo uma abordagem preventiva e transparente (Bioni, 2019; Martins, 2021).

Como sugestão, este trabalho propõe que a legislação sobre dados seja atualizada, ao menos para constar os conceitos afetos ao *profiling*, como, definição de perfis, perfilização, dados de coletividade entre outros conceitos de ordem indeterminada e discutidos apenas pela doutrina brasileira. Após esses conceitos poderia se iniciar discussões setorizadas, mas específicas às diferentes formas de tratamento automatizado de dados e a partir disto pensar soluções enquanto uma matéria de interesse público. As iniciativas voltadas ao reequilíbrio entre a relação usuários e plataforma serão abordadas na Seção 6.

4.2 Breve histórico da formação da empresa Meta Platform Inc

A Meta Platforms, Inc., originalmente fundada como Facebook, Inc., surgiu em 4 de fevereiro de 2004 nos Estados Unidos, idealizada por Mark Zuckerberg e seus colegas de quarto, Eduardo Saverin, Andrew McCollum, Dustin Moskovitz e Chris Hughes, na Universidade de Harvard (FM2S, 2024).

Inicialmente tratava-se de uma comunidade restrita aos alunos de Harvard, onde os usuários poderiam interagir e encontrar pessoas próximas através da ferramenta, além de facilitar a organização de festas, trabalhos, grupos de estudos entre outras funcionalidades do universo acadêmico. A rede rapidamente se expandiu para outras universidades, chegando a duas mil universidades em dois anos. Logo depois se tornou acessível ao público em geral, marcando o início de uma trajetória de crescimento acelerado (FM2S, 2024).

A partir de 2005, com o aporte de investidores a empresa consolidou sua posição no mercado e passou a inovar em funcionalidades: em 2006, lançou o News Feed, que permitia aos usuários acompanharem atualizações de amigos em tempo real, e em 2009, introduziu o botão “Curtir”, recurso que se tornou um dos símbolos da cultura digital contemporânea. (FM2S, 2024)

Sobre o recurso “curtir” este tem papel fundamental no desenvolvimento da cultura das redes sociais com se conhece hoje, pois na prática atua como um termômetro medidor de interesse e inferência de dados, o que torna um botão, aparentemente inofensivo, uma das atualizações mais revolucionárias das redes sociais (Pereira; Pontes; Tozatto 2022). Neste sentido vejamos como os autores, João Vitor Nunes Pereira, Ritiele Queles Pontes e Alessandra Tozatto abordam a importância do like na plataforma:

O “like” atua nesse contexto como um “medidor” de conteúdo, onde quanto mais likes se tem melhor teoricamente é o conteúdo, com o passar do tempo o valor das coisas e das pessoas passou a ser medido pela quantidade de likes que ela tem, comportamento que rapidamente se vinculou com os níveis de satisfação de cada pessoa, dessa forma a satisfação plena só é alcançada se as publicações nas redes agradarem muitas pessoas e elas retribuírem com likes, o que pode ser entendido como um qualificador (Pereira; Pontes; Tozatto, 2022).

O Facebook, como rede social, tornou-se rapidamente a principal plataforma de interação online da empresa. Em 2014 contava com 70% dos brasileiros conectados à internet e em 2016 aparecia entre os sites mais acessados no mundo, ocupando a segunda posição. A empresa então passou a diversificar seus produtos, adquirindo aplicativos estratégicos como Instagram (2012) e WhatsApp (2014), além do Messenger e da Oculus, expandindo sua atuação para além das redes sociais tradicionais e entrando no mercado de realidade virtual e aumentada (Meta Platforms, 2025)

Em 2010, o Facebook foi eleito a empresa mais inovadora do mundo, outro marco importante da empresa, foi o fato de ser a primeira rede social a conseguir êxito ao implementar anúncios publicitários, além de criar moedas virtuais para utilização em jogos e aplicativos, o que também rendeu uma fonte de geração de recursos, abrindo caminho para o que seria hoje um dos modelos de negócios mais lucrativos da atualidade (O Facebook, 2011).

Em 28 de outubro de 2021, a empresa anuncia a mudança do nome, de Facebook, Inc. para Meta Platforms Inc., refletindo a nova estratégia corporativa voltada para o desenvolvimento do chamado “metaverso”, um ambiente virtual imersivo e colaborativo, considerado pela empresa como o próximo estágio da conexão social (FM2S, 2024; Palmeira, 2021).

O Instagram vem se consolidando como uma das redes com maior aderência no mundo, totalizando mais de dois bilhões de usuários ativos até 2024, dos quais cerca de 134,6

milhões são de consumidores brasileiros, conseguindo alcançar aproximadamente 62% da população com anúncios (Jornal Digital Recife, 2024; Gonçalves, 2025).

Em 2024, a *Opinion Box*, empresa que realiza pesquisas *online* sobre redes sociais para fins de *insight*, entrevistou 2.047 usuários brasileiros, maiores de 16 anos, de todas as faixas etárias, regiões e classes sociais para entender as preferências dos usuários. A pesquisa revela que 93% dos usuários acessam o Instagram pelo menos uma vez ao dia, sendo que 57% entram várias vezes ao longo do dia e 17% chegam a manter o aplicativo aberto o dia inteiro (Gonçalves, 2025).

A pesquisa também apresenta dados de consumo em que 72% dos usuários informaram já ter comprado algum produto ou serviço pela plataforma, seja por meio de anúncios, recomendações de influenciadores ou postagem das próprias marcas (Gonçalves, 2025).

Já o Facebook (rede social), em que pese ter números menores, ainda é utilizado por aproximadamente 112 milhões de usuários brasileiros, posicionando o país como o quarto maior mercado da plataforma e com previsão de aumento de 17,2 milhões de usuários, chegando a 144, 81 milhões até 2028 segundo dados da empresa de marketing digital RD Station (Rodrigues, 2024).

Esses números posicionam o Brasil entre os maiores mercados globais para as plataformas da Meta, evidenciando forte presença da empresa na vida digital da população e seu papel fundamental na dinâmica das comunicações, entretenimento e consumo de informação no país (Veríssimo; 2024).

Estudiosos do assunto atribuem tal popularidade ao fato de que as redes sociais funcionam como espaços de socialização, pertencimento e construção de identidade, especialmente em sociedades marcadas por alta sociabilidade como a brasileira (Lima; Nogueira, 2023).

Em que pese os números expressivos e a grande aderência dos produtos da empresa meta, a trajetória da empresa também é marcada por um histórico problemático no que se refere ao uso indevido de dados e violação de privacidade, constantemente sendo alvo de investigações e questionamentos por parte de órgãos judiciais e administrativos de diversos países envolvendo o Brasil (Bioni, 2019; Doneda, 2006; ANPD, 2024).

Um dos mais emblemáticos que envolve diretamente a questão da perfilização é caso Cambridge Analytica, em 2018, que será objeto de item próprio nesta pesquisa. Todavia outros episódios uso indevido de dados foram registrados, ainda em 2018 foram recebidas

denúncias de que o Facebook vinha coletando, de forma sistemática, registros de chamadas telefônicas e mensagens SMS de usuários do aplicativo Messenger, especialmente em dispositivos Android (BBC News Brasil, 2018).

A descoberta ocorreu quando usuários, ao baixarem seus próprios arquivos de dados armazenados pela plataforma, identificaram históricos detalhados de ligações (incluindo números, duração, horários e nomes dos contatos) e mensagens de texto, abrangendo até mesmo contatos que já não estavam mais salvos em seus aparelhos. O caso ganhou grande repercussão internacional após os relatos de usuários e foi denunciada em 2018 (BBC News Brasil, 2018).

Como justificativa empresa alegou que a coleta era autorizada pelos próprios usuários que consentiam com a prática no momento da instalação dos aplicativos, através de permissões genéricas e demasiadamente amplas, o Facebook alegou ainda que possuía um legítimo interesse na coleta e que o objetivo seria aprimorar a experiência do usuário. Deste episódio não há registro de sanções efetivamente aplicadas, entretanto o fato contribuiu para a intensificação dos debates sobre políticas de privacidade e na forma de solicitação de permissões em aplicativo (Bioni, 2019; BBC News Brasil, 2018).

Além da internalização de dados dos usuários em suas bases de dados a empresa também já esteve no centro de discussões sobre vazamento de dados. Em abril de 2021, foi divulgado que dados pessoais de aproximadamente 533 milhões de usuários do Facebook, provenientes de mais de 100 países, incluindo o Brasil, haviam sido expostos em fóruns abertos da internet. Entre as informações vazadas estavam nomes completos, números de telefone, cidades de origem, profissões, estados civis e, em alguns casos, obtidos por meio da exploração de uma vulnerabilidade na funcionalidade de busca por contatos do Facebook que permitiu a consulta pública, facilitando ataques de engenharia social e outras práticas ilícitas (Lomas, 2018).

A recorrência desses episódios demonstra a centralidade dos desafios éticos, jurídicos e sociais enfrentados pela empresa e reforça a necessidade de mecanismos regulatórios robustos para garantir a proteção dos direitos de personalidade no contexto das redes sociais.

4.3 Google e o legado do superávit comportamental

Ainda no cenário das *big techs*, o Google merece atenção especial, por inaugurar a economia de dados no modelo em que se conhece hoje (Zuboff, 2020). Shoshana Zuboff traça o paralelo de que o Google está para o capitalismo de vigilância, tal qual a Ford e a General Motors estão para o capitalismo gerencial na produção em massa, atribuindo à empresa o pioneirismo por operar em uma nova lógica de acumulação com leis de movimento próprias, que não rompe com as leis capitalistas consagradas mas incorpora ao seus meios de produção sistemas mais complexos baseados em inteligência de máquina, que culminou em um poder (chamado pela autora de poder instrumentário) sem precedentes, que serviu como um alicerce para o capitalismo de vigilância (Zuboff, 2020, p.105).

Fundado nos anos noventa pelos estudantes de pós-graduação Larry Page e Sergey Brin, da Universidade de Stanford, na Califórnia, Estados Unidos. O Google inicia como uma pesquisa acadêmica, que buscava desenvolver um motor de busca mais eficiente do que os existentes na época, analisando a relevância das páginas por meio dos backlinks³⁴ e não apenas pela contagem de palavras-chave³⁵.

A empresa observou que cada busca realizada produzia recursos de dados colaterais inéditos como o padrão dos termos de busca, ortografia, pontuação, tempo de visualização em uma página, padrões de cliques e localização, que eram armazenados pela plataforma, mas a princípio não tinham uma destinação de uso, eram considerados apenas dados acidentais (Zuboff, 2020. p.106).

A virada de chave acontece quando Amit Patel, também estudante da pós-graduação em Stanford, com especial interesse em mineração de dados, tem o *insight* de analisar esses dados acidentais, acreditando que esses dados forneceriam sensor de comportamento que alimentariam o sistema de aprendizagem dos mecanismos de busca permitindo a criação de produtos inovadores como, verificação de ortografia, tradução e reconhecimento de voz (Zuboff, 2020, p.106).

Os dados que antes eram apenas um material residual, passaram a ser utilizado para aperfeiçoar o motor de busca do Google e eram reinvestidos na experiência dos usuários para

³⁴ Backlinks são links de entrada de outros sites para uma página da web, funcionando como referências que indicam relevância e autoridade para mecanismos de busca.

³⁵ Palavras-chave são termos compostos por uma ou mais palavras que resumem o tema principal de um conteúdo, sendo utilizados para otimizar o posicionamento em resultados de busca

melhorar a rapidez, relevância e precisão dos resultados, formando um ciclo de *reinvestimento do valor comportamental* (Zuboff, 2020).

Com esta prática o Google conseguiu atingir um nível de excelência na performance do serviço de mecanismo de busca, mas ainda não era rentável, as informações obtidas eram reinvestidas na melhoria dos serviços, não havia uma troca econômica, preço ou lucro, ainda não existia um produto a ser vendido, e consequentemente não havia a acumulação de capital. Usuários e plataforma se relacionavam em um equilíbrio de poder.

O fato de usuários precisarem da busca quase tanto quanto a busca precisava dos usuários criava um equilíbrio de poder entre o Google e seu público. As pessoas eram tratadas como fins em si, os sujeitos de um não mercado, um ciclo contido em si próprio que se alinhava à perfeição com a missão do Google de “organizar a informação do mundo, tornando-a universalmente acessível e útil (Zuboff, 2020. p.113).

Com os altos investimentos e pouca receita gerada pelas startups, incluindo a Google, em abril de 2000 acontece o estouro da chamada *bolha das empresas ponto com*. A economia da internet entra em recessão, com diversas startups antes tidas como promissoras entrando em declínio. Em que pese a Google ainda ser considerada a melhor empresa entre as ferramentas de busca, a pressão por lucro se intensifica, não bastava potencial, era necessário mostrar resultados (Zuboff, 2020. p.113).

Diante deste senso de emergência por lucros, Google passaria a investir na combinação entre buscas e anúncios, utilizando como vantagem competitiva uma matéria prima já extraída pela empresa a custo zero, os dados comportamento que eram coletados de forma acidental e antes utilizados apenas para a otimização dos serviços. A partir daí este *Know How* seria utilizado, além do aprimoramento dos serviços, para combinar anúncios com busca, a intenção era gerar propagandas que fossem relevantes para os usuários, direcionando anúncios específicos para usuários específicos, assim identificados com base nos dados armazenados pelo mecanismo de busca da Google (Zuboff, 2020. p. 117).

Em outras palavras, o Google não faria mais mineração de dados comportamentais estritamente para melhorar o serviço para seus usuários, e sim para ler as mentes destes a fim de combinar anúncios com seus interesses, que, por sua vez, eram deduzidos dos vestígios colaterais do comportamento on-line. Com o acesso exclusivo do Google aos dados

comportamentais, seria possível então saber o que um indivíduo específico, num tempo e espaço específicos, estava pensando, sentindo e fazendo (Zuboff, 2020, p. 122).

Ao utilizar os dados de comportamento para além da melhora de performance esses dados seriam utilizados para melhorara a lucratividade do Google e de seus anunciantes. A Google tinha mais dados comportamentais do que o necessário para servir aos usuários. Este *além* constituía um superávit, o *superavit comportamental* que possibilitaria o lucro constante e exponencial exigido pelo mercado. Como resultado deste movimento, os anúncios da Google foram considerados mais eficazes do que a maioria das propagandas *on-line* da época (Zuboff, 2020. p. 118-120).

No lugar de cobrar pelo número de visualizações dos anúncios a nova métrica de precificação da Google passou a se basear em “taxas de cliques” que eram constantemente aprimoradas e, portanto, mais eficazes em predições, quanto melhores as predições maiores as taxas de click, em pouco tempo os leilões automatizados da Google acumularam bilhões e mais tarde trilhões de anunciantes.

Após a descoberta deste novo modelo de negócio a partir da publicidade dirigida, a Google continuou em expansão e em 2015 criou a *holding* Alphabet Inc. que passou a ser a empresa controladora, mantendo o nome Google apenas para os produtos e serviços de buscas e anúncios.

Desde então a empresa passou a diversificar seus produtos, adquirindo empresas de produtos informatizados para casa, soluções de gerenciamento de anúncios, software de buscas inteligentes e análise de dados, aplicativos de navegação móvel (Waze) e dispositivos de aplicativos *fitness*. A expansão para diferentes seguimentos permite novas formas de captação de dados em diversas camadas do comportamento humano (Cassino; Souza; Silveira, 2021, p. 72 - 73)

Mais de duas décadas depois da descoberta que revolucionária o mercado e pavimentaria o capitalismo de vigilância a Google, agora Alphabet se tornou um dos maiores conglomerados de tecnologia do mundo, com capitalização de mercado de 1,4 trilhão de dólares em fevereiro de 2021 se mantendo como uma das empresas mais influentes da economia da informação.

4.4 O capitalismo de vigilância

No contexto do objeto deste trabalho a compreensão do capitalismo de vigilância e da datificação da vida são fundamentais para o entendimento do problema de pesquisa apresentado. Tais institutos atuam de forma codependentes, como parte de uma estrutura, uma engrenagem com diversos atores, na qual se incluem as redes sociais, e diversas ferramentas necessárias ao seu funcionamento, na qual se inclui a perfilização. Esses fenômenos reconfiguram as dinâmicas de poder e consequentemente abrem espaço para outras formas de violação de direitos (Zuboff, 2019; Bioni, 2019).

A datificação da vida, ao transformar cada comportamento humano em dados quantificáveis, cria a base essencial para a prática da perfilização. Essa última, por sua vez, utiliza esses dados coletados para construir perfis detalhados dos usuários, que são fundamentais para alimentar os sistemas de predição e modulação comportamental característicos do capitalismo de vigilância.

Assim, a perfilização emerge como uma extensão natural e necessária da datificação, pois é por meio dela que os dados ganham significado prático e instrumental, permitindo que as empresas antecipem comportamentos e moldem mercados futuros. Essa conexão evidencia a interdependência entre os processos, reforçando que a datificação não é um fim em si mesma, mas um passo crucial para a geração de valor econômico e controle social.

Em primeiro plano, observa-se a prática da datificação da vida, por meio da qual todo comportamento humano é registrado e transformado em *superávit comportamental*. Contudo, essa dinâmica, não se esgota em si mesma, sendo apenas uma das peças de uma engrenagem maior, qual seja o capitalismo de vigilância.

Neste contexto a perfilização é técnica praticada pelas redes sociais para a geração do insumo que possibilita uma das finalidades do capitalismo de vigilância, qual seja, a predição, possibilitando às empresas se antecipar, criar e prever mercados futuros, a partir do monitoramento do comportamento humano. Nesse sentido, é necessário considerar os institutos de perfilização, datificação, modulação de comportamento e capitalismo de vigilância como camadas interdependentes, nas quais o tratamento de dados possui natureza instrumental e não finalística.

A compreensão aprofundada dessas dinâmicas é fundamental para o problema central do trabalho, que busca analisar a compatibilidade da prática de perfilização nas redes sociais da Meta Platforms Inc. com os princípios do livre desenvolvimento da personalidade e da

autodeterminação informativa. Ao destacar como a datificação e a perfilização operam como mecanismos intrinsecamente ligados dentro do capitalismo de vigilância, o estudo evidencia as formas pelas quais esses processos impactam diretamente os direitos dos usuários, ampliando a reflexão sobre os desafios regulatórios e as lacunas existentes na legislação brasileira, especialmente no que tange à proteção efetiva da autonomia dos indivíduos no ambiente digital.

Silveira, Souza e Cassino, ao estudarem o colonialismo de dados, explicam que assim como outras formas de extração, como o ouro e o petróleo, que necessitavam de toda uma estrutura para que pudessem operar, como plataformas de perfuração e maquinários apropriados, para que fossem possíveis a retiradas dos ativos, os dados demandam infraestruturas tecnológicas como data centers, cookies³⁶, algoritmos³⁷ para coleta, processamento e monetização, assim o avanço tecnológico foi a ponte que permitiu a montagem dessa estrutura (Silveira; Souza; Cassino, 2021).

Zuboff (2021) considera o capitalismo de vigilância como uma mutação do capitalismo tradicional e desenvolve sua teoria sob a perspectiva de um modelo globalizado, cujo funcionamento e estrutura ultrapassam fronteiras nacionais e integrando diferentes regiões do mundo em uma rede interconectada. Neste item conservaremos o entendimento de que o capitalismo de vigilância é uma mutação do capitalismo tradicional, entretanto do ponto de vista geográfico limitaremos a análise aos países periféricos levando em consideração a posição ocupada pelo Brasil.

Partindo dessa perspectiva, observa-se que, no caso brasileiro, a posição periférica no mercado global de dados reforça a vulnerabilidade estrutural dos usuários e do próprio Estado, que se veem dependentes de infraestruturas e lógicas de negócios definidas por grandes corporações estrangeiras (Silveira; Souza; Cassino, 2021). A exportação de dados e a ausência de soberania tecnológica agravam o cenário de assimetria de poder e submissão, dando espaço para novas formas de colonização, agora no ambiente digital.

³⁶ Cookies são pequenos arquivos de texto criados por sites e armazenados no navegador do usuário durante a navegação na internet. Esses arquivos contêm informações como preferências de navegação, dados de autenticação ou itens adicionados a um carrinho de compras, permitindo que o site reconheça o usuário em visitas futuras e mantenha determinadas configurações ou sessões ativas. O funcionamento dos cookies está relacionado ao registro e à recuperação dessas informações pelo próprio site ou por terceiros, de acordo com as interações realizadas pelo usuário ao acessar diferentes páginas (G1, 2024).

³⁷ Algoritmo pode ser definido como uma sequência finita de passos, logicamente ordenados, destinados à resolução de um problema específico. Cada passo do algoritmo corresponde a uma instrução clara e precisa, que deve ser executada de forma sistemática até que se alcance o resultado desejado. No contexto da computação, os algoritmos são fundamentais para o desenvolvimento de programas, pois estruturam o processamento das informações e orientam a execução das tarefas pelas máquinas de maneira eficiente e previsível (Ferrari, 2012).

Antes de adentrarmos as discussões, é importante apresentar dois breves esclarecimentos que contribuem para a precisão conceitual do trabalho. O primeiro refere-se à nomenclatura: embora o termo "capitalismo de vigilância" seja frequentemente associado a estudos sobre "economia de vigilância", opta-se aqui por utilizar o primeiro por sua especificidade. Enquanto "economia de vigilância" pode abranger análises mais amplas e difusas, o "capitalismo de vigilância" destaca-se por abordar as estruturas de poder e as dinâmicas mercadológicas centrais ao objeto desta pesquisa.

O segundo esclarecimento diz respeito à relação entre capitalismo de vigilância e tecnologia. Apesar da conexão intrínseca entre ambos, é fundamental notar que não se confundem. Como destaca Zuboff (2019, p. 32): "O capitalismo de vigilância não é tecnologia; é uma lógica que permeia a tecnologia e a direciona numa ação. O capitalismo de vigilância é uma forma de mercado que é inimaginável fora do meio digital, mas não é a mesma coisa que 'digital'".

A partir desse entendimento, comprehende-se que o capitalismo de vigilância representa uma nova ordem econômica, na qual a experiência humana é transformada em matéria-prima para práticas de extração, predição e comercialização de comportamentos. O pioneirismo desse modelo é atribuído ao Google, cuja atuação vai além da simples coleta de dados, englobando a criação de mercados futuros baseados na antecipação e modulação de ações humanas.

Diferentemente do capitalismo tradicional, em que o poder reside no domínio dos meios de produção, o capitalismo de vigilância exerce seu poder por meio do chamado poder instrumentário. Trata-se de uma forma de influência que opera através de instrumentos tecnológicos, algoritmos, sistemas automatizados e arquitetura digital, capazes de modular decisões, preferências e ações de indivíduos ou grupos. Não há coerção física direta, mas sim intervenções sutis e contínuas, que influenciam comportamentos e subjetividades de maneira instrumental, tornando a modulação comportamental o principal resultado almejado nesse novo paradigma.

Zuboff (2019) nomeia de *poder instrumentário*, como uma forma de poder que atua por meio de instrumentos tecnológicos para moldar humano, suas decisões e até mesmo subjetividade humana, entretanto o na forma instrumentária, não há coerção física, mas sim uma capacidade de moldar decisões, preferências e ações por meio de sistemas automatizados, algoritmos e arquitetura digital, que conseguem influenciar os indivíduos, não há coerção direta, mas sim intervenções sutis, capazes de influenciar uma determinada pessoa,

ou grupo de pessoas, a fazerem ou não algo, o poder instrumentário é então a finalidade, o resultado que se deseja no capitalismo de vigilância.

O poder instrumentário conhece e molda o comportamento humano em prol das finalidades de terceiros. Em vez de armamentos e exércitos, ele faz valer sua vontade através do meio automatizado de uma arquitetura computacional cada vez mais ubíqua composta de dispositivos, coisas e espaços “inteligentes” conectados em rede (Zuboff, 2019, p. 23)

Já os meios de modificação comportamental são os mecanismos e técnicas utilizados para esta finalidade, além das estratégias utilizadas, tais como: sistemas de recomendação, personalização de conteúdo, designers persuasivos, e nessas técnicas, se inclui a perfilização, técnica que permite a geração do insumo necessário à atuação de um meio de modificação comportamental, a perfilização funciona então como o roteiro que irá orientar os meios de modificação.

Percebe-se então que os meios de modificação comportamental estão para o capitalismo de vigilância tal qual os meios de produção estavam para o capitalismo tradicional, e em ambos, tais instrumentos de domínios, são centralizados por um pequeno grupo, desta vez representados pelas empresas de tecnologia, as chamadas *big techs*. Aprofundaremos a discussão sobre esta concentração de poder no item 5.2 dedicado a análise do colonialismo de dados e o monopólio GAFAM.

Todavia tal relação se desenvolve de forma assimétrica, como uma via de mão única, em que o Brasil exporta um grande volume de dados, sem que haja algum retorno econômico e/ou tecnológico para o país (Cassino; Souza; Silveira, 2021). Como resultado, forma-se entre os países (Brasil x Estados Unidos) uma espécie de neocolonialismo, caracterizado pela continuidade das relações de dominação e exploração de países ricos (principalmente os industrializados) e países mais pobres ou em desenvolvimento (Faustino; Lippold, 2023).

Transformar vidas em commodities e controlá-las por meio da vigilância não é algo novo na história da humanidade e já vem sendo discutido por autoras como Simone Browne. No entanto, é importante notar que, diferentemente do colonialismo histórico, o colonialismo de dados não precisa utilizar a violência física para se apropriar dos diversos aspectos da vida humana, pois pode operar “por meios distintos de força para se certificar que há colaboração dos sistemas emaranhados de extração da vida diária (Machado, 2021, p. 53).

Nesse contexto, a dinâmica global de circulação de dados evidência não apenas desigualdades econômicas e tecnológicas, mas também aprofunda dependências estruturais entre países centrais e periféricos. A centralização do controle sobre os fluxos informacionais por parte das grandes corporações tecnológicas reforça a posição de vulnerabilidade dos países em desenvolvimento, como o Brasil, e limita sua capacidade de participação ativa e autônoma na economia digital.

O capitalismo de vigilância estrutura-se em três pilares principais: (i) A coleta massiva de dados e criação de perfis comportamentais, (ii) A manipulação algorítmica e modulação do comportamento, e (iii) A normalização da vigilância com ausência de transparência regulatória. Esse modelo não apenas redefine as dinâmicas do mercado, mas também impõe desafios inéditos à democracia, à privacidade e aos direitos fundamentais.

4.4.1 Capitalismo de vigilância e o livre desenvolvimento da personalidade

O ser humano está em constante relação de influência recíproca com tudo aquilo com que interage, sejam pessoas ou objetos. No ambiente digital, essa dinâmica se mantém, mas com a presença de um novo agente: o algoritmo. Esse sistema de processamento de dados utiliza uma vasta gama de informações sobre o usuário para determinar como as plataformas digitais irão se comportar, quais conteúdos serão apresentados e quais permanecerão ocultos.

O livre desenvolvimento da personalidade abrange tanto a proteção da integridade pessoal quanto a garantia de liberdade geral de ação, dimensões que podem ser violadas quando o poder de decisão sobre a própria vida é transferido para sistemas algorítmicos já que o tratamento automatizado de dados pessoais, especialmente em larga escala, tem o potencial de gerar externalidades negativas, como autocensura, customização comportamental, que limitam a liberdade de ser e agir conforme a própria vontade.

Para que o livre desenvolvimento da personalidade ocorra de maneira plena o indivíduo deve sofrer o mínimo de intervenção possível em suas ações. Por esse motivo, entendemos aqui neste trabalho que os *meios de modificação comportamental*, com o nível de opacidade em que são empregados nas redes sociais e somados às lacunas referentes aos limites de privacidade, é o que faz com que a técnica de *Profiling* seja incompatível com o princípio do livre desenvolvimento, devido ao seu potencial de interferir na percepção crítica dos usuários ao ponto de influenciar seu comportamento.

Desta forma, os algoritmos de perfilização atuam como o mediador de nossas escolhas e percepções, ocupando a figura de um terceiro, na construção da identidade narrativa, se antes a narrativa era construída por um “eu” e um “outro” (Ricoeur; 1991) agora o diálogo destas partes passa a ser mediado por um terceiro ator, que escolhe quais informações e em qual quantidade acontecerá este contato.

É nesse contexto que surge o fenômeno conhecido como *filtro bolha*, resultado da filtragem algorítmica da informação, pelo qual os usuários passam a acessar conteúdos cada vez mais personalizados, baseados em suas preferências e comportamentos anteriores, ao mesmo tempo em que têm o acesso a informações divergentes restrinrido (Santana; Neves 2022).

Os *filtros bolha* constituem mecanismos algorítmicos implementados por plataformas digitais que, ao personalizarem o conteúdo exibido a partir dos dados e preferências dos usuários, acabam restringindo o acesso a informações divergentes e reforçando visões de mundo já existentes. Esse processo fragmenta o fluxo informacional, criando ambientes personalizados nos quais o indivíduo é exposto predominantemente a conteúdos que confirmam suas crenças, dificultando o contato com perspectivas alternativas e contribuindo para a polarização e a desinformação no ambiente digital (Silva; Silva, 2024, p. 5).

Como discutem Santana e Neves (2022), essa modulação algorítmica gera ambientes informacionais controlados, nos quais o fluxo de informações é direcionado de acordo com propósitos específicos das plataformas, o meio de modificação comportamental escolhido e empregado de acordo com a finalidade pretendida, em uma manobra estruturada para interesse de terceiros (Zuboff, 2019: Santana e Neves, 2022).

A articulação entre a teoria do capitalismo de vigilância, de Shoshana Zuboff, e a filosofia da identidade de Paul Ricoeur permite compreender como a perfilização impacta a formação da subjetividade contemporânea no ambiente digital. Zuboff demonstra que o capitalismo de vigilância expropria não apenas dados, mas também a capacidade de os indivíduos construírem narrativas próprias sobre si mesmos, ao substituir a autodeterminação por modelos preditivos e influências comportamentais. Nesse contexto, a identidade deixa de ser o resultado de uma vida examinada, reflexiva e dialógica, para se tornar objeto de manipulação externa.

Essa articulação teórica dialoga diretamente com o objeto da pesquisa ao evidenciar que a perfilização não apenas recolhe dados, mas interfere na construção da identidade narrativa dos usuários, comprometendo sua capacidade de autodeterminação e livre

desenvolvimento da personalidade. A relevância prática dessas discussões reside na necessidade de avaliar criticamente as práticas das redes sociais da Meta Platforms Inc., considerando seus efeitos concretos sobre os direitos fundamentais previstos na LGPD.

Ao integrar essas perspectivas, o trabalho contribui para a formulação de propostas regulatórias que busquem equilibrar inovação tecnológica e proteção dos direitos individuais e coletivos, destacando a urgência de mecanismos que promovam transparência, controle e participação dos usuários no ambiente digital.

Paul Ricoeur, em sua obra *O Si-mesmo como Outro*, propõe que a identidade narrativa é fundamental para a constituição do sujeito, pois integra experiências, memórias e projetos futuros em uma história coerente de si mesmo. A narrativa de si não é apenas uma ferramenta estética, mas sobretudo ética, pois permite ao indivíduo avaliar suas ações e relações com os outros, mantendo a promessa como atestação de si mesmo. Quando a narrativa pessoal é substituída por constructos algorítmicos, o sujeito perde a capacidade de se reconhecer em sua própria história, comprometendo a integridade e a autonomia moral.

A análise conjunta dessas abordagens revela uma tensão entre a lógica instrumental do capitalismo de vigilância, que objetifica o indivíduo como fonte de dados, e a perspectiva hermenêutica de Ricoeur, que valoriza a narrativa como elemento constitutivo da identidade. Esse cruzamento teórico aponta para a necessidade de proteger a identidade narrativa dos indivíduos, garantindo que o livre desenvolvimento da personalidade não seja subordinado aos imperativos econômicos das plataformas digitais.

Ao analisar os fundamentos econômicos, tecnológicos e sociais que sustentam a economia de dados e o capitalismo de vigilância, bem como os impactos concretos da prática de *profiling*, especialmente nas redes sociais da Meta Platforms Inc., evidencia-se a complexidade e a profundidade dos desafios impostos à sociedade contemporânea.

Tais desafios extrapolam a esfera individual, atingindo dimensões coletivas e institucionais. Diante desse cenário, torna-se imprescindível avançar a discussão para os desafios jurídicos e regulatórios que emergem da consolidação dessas práticas.

5 DESAFIOS GLOBAIS E PERSPECTIVAS REGULATÓRIAS DO *PROFILING* EM REDES SOCIAIS

Ao longo do trabalho foram feitos alguns levantamentos teóricos para demonstrar o potencial de manipulação do *profiling* e de como isto pode ser nocivo ao livre desenvolvimento da personalidade. Nesta seção a pesquisa traz o caso da Cambridge Analytica, como um exemplo paradigmático amplamente estudado pela doutrina nacional e internacional para discutir a manipulação do comportamento em massa através das redes sociais.

5.1 O caso Cambridge Analytica

Fundada em 2013, a Cambridge Analytica se apresentava no mercado como uma empresa de consultoria política especializada em gestão de campanhas eleitorais globais, análise de dados, segmentação de audiência e comunicação estratégica baseada em ciência de dados (Silva, 2024).

A atuação da empresa se dava através dos serviços de coleta, cruzamento e análise de dados de diversas fontes digitais (como Facebook, Google, Twitter, Instagram e WhatsApp), extraíndo as informações destes perfis com o objetivo de criar perfis psicológicos detalhados de eleitores e, a partir disso, direcionar campanhas políticas personalizadas (Silva, 2024).

A empresa ganhou notoriedade durante a eleição presidencial dos Estados Unidos em 2016, quando foi contratada para atuar na campanha do então candidato Donald Trump, do Partido Republicano, que concorria com a candidata do partido Democrata, Hillary Clinton. O objetivo da empresa era utilizar técnicas avançadas de análise de dados e *microtargeting*³⁸ para influenciar o comportamento dos eleitores indecisos de segmentos específicos da população e consequentemente promover o candidato republicano (Silva, 2024).

A Meta Platforms Inc., foi peça central do episódio, pois foi a partir de suas plataformas que a Cambridge Analytica obteve acesso indevido aos dados pessoais de cerca

³⁸*Microtargeting* é uma técnica de comunicação que utiliza o cruzamento de grandes volumes de dados pessoais para identificar e segmentar grupos específicos de indivíduos, permitindo o direcionamento de mensagens personalizadas com alto grau de precisão. Essa abordagem se diferencia da comunicação de massa ao priorizar a qualidade da segmentação em vez da quantidade de pessoas atingidas.

de 87 milhões de usuários em diversos países, incluindo o Brasil. A coleta foi viabilizada por meio do aplicativo “*thisisyour digital life*”, desenvolvido pelo pesquisador Aleksandr Kogan, que se apresentava aos usuários como um serviço de testes de personalidade com base na técnica OCEAN score³⁹, desenvolvida na década de 1980 que classifica a personalidade humana em cinco grandes dimensões fundamentais (Silva, 2024).

A técnica *OCEAN score*, originalmente desenvolvida e validada no campo da psicologia para mensuração de personalidade em cinco grandes traços/categorias, sendo elas: (i) Abertura; (ii) Conscienciosidade; (iii) Extroversão; (iv) Amabilidade e (v) Neuroticismo. A estratégia da empresa consistia em adaptar a OCEAN score para fins políticos, utilizando os perfis universais definidos para criar estratégias que pudessem influenciar eleitores indecisos a votar no candidato do partido republicano, Donald Trump, utilizando as redes sociais da empresa Meta como meio para a obtenção de respostas (Aguiar, 2021; Santos, 2025; Ayres Pinto; Moraes, 2020).

A empresa coletou dados psicométricos e comportamentais de usuários do Facebook, correlacionando respostas a questionários com atividades na plataforma, como curtidas, compartilhamentos e interações. E a partir da inferência de informações construiu os perfis psicográficos⁴⁰ detalhados, que possibilitaram a segmentação do eleitorado em grupos com motivações, valores e vulnerabilidades distintas (Aguiar, 2021; Santos, 2025; Ayres Pinto; Moraes, 2020).

A partir dessa segmentação, algoritmos direcionavam mensagens políticas personalizadas, ajustadas ao perfil psicológico de cada grupo, intensificando o potencial persuasivo das campanhas e otimizando a influência sobre o comportamento eleitoral ao permitir um direcionamento do conteúdo eleitoral de forma altamente personalizada. Ao aceitar participar, os usuários autorizavam o acesso não só aos próprios dados, mas também aos dados de seus amigos na rede, sem o devido consentimento destes. (Aguiar, 2021; Santos, 2025; Ayres Pinto; Moraes, 2020).

³⁹ O OCEAN score, também conhecido como modelo dos Cinco Grandes Fatores de Personalidade (Big Five), é uma técnica psicométrica amplamente reconhecida e validada internacionalmente para avaliação da personalidade humana. O modelo foi desenvolvido por Paul Costa e Robert McCrae no National Institutes of Health (NIH), nos Estados Unidos, a partir da década de 1980, e avalia cinco dimensões fundamentais: abertura a experiências, conscienciosidade, extroversão, amabilidade e neuroticismo. Normalmente a técnica é utilizada principalmente para avaliar traços de personalidade em contextos de psicologia organizacional, por exemplo, nas áreas de recursos humanos e recrutamento e seleção de candidatos.

⁴⁰ Perfis psicográficos são descrições detalhadas que buscam compreender os aspectos comportamentais e psicológicos de um grupo de indivíduos, indo além de características demográficas tradicionais como idade, gênero ou renda. Esses perfis são construídos a partir de elementos como interesses, valores, atitudes, estilo de vida, personalidade e motivações, permitindo identificar não apenas quem são os indivíduos, mas principalmente por que eles agem de determinada maneira.

Embora o Facebook alegasse desconhecimento sobre o uso indevido dos dados, investigações posteriores apontaram falhas graves em suas políticas de privacidade e fiscalização, culminando em processos judiciais e acordos bilionários para reparação dos danos (Fornasier; Beck, 2020; Silva, 2024)

A estratégia foi considerada bem-sucedida do ponto de vista da campanha, pois Trump saiu vitorioso nas eleições, mas não há consenso acadêmico sobre o grau exato de impacto da Cambridge Analytica no desempenho eleitoral de Donald Trump, mas relatório internos da empresa a estratégia utilizada gerou um aumento médio de 3% na favorabilidade de Trump e aumentaram em 2% o número de votos por correspondência em públicos-alvo estratégicos. (Cadwalladr; Graham-Harrison, 2018).

Apesar da ausência de dados precisos sobre a extensão do impacto do caso Cambridge Analytica nas eleições de diferentes países, o episódio tornou-se um paradigma global sobre os riscos associados à exploração política de dados pessoais em plataformas digitais. O escândalo levantou questionamentos profundos sobre a eficácia dos mecanismos de proteção de dados e a integridade dos processos democráticos, sendo amplamente repercutido por veículos internacionais e nacionais de prestígio, como *The Guardian*, *The New York Times*, *BBC News* e *Folha de S. Paulo* (Cadwalladr, 2018; Rosenberg; Confessore; Cadwalladr, 2018; BBC News, 2018; Folha de S. Paulo, 2018).

A análise do caso Cambridge Analytica revela, de forma concreta, como a manipulação algorítmica e a extração massiva de dados impactam diretamente direitos fundamentais, como a autodeterminação informativa e o livre desenvolvimento da personalidade, temas centrais do objeto desta pesquisa.

O episódio evidencia a necessidade de regulação mais robusta e transparente, pois demonstra que a ausência de mecanismos eficazes de controle e fiscalização pode resultar em violações substanciais à privacidade, à liberdade de escolha e à integridade das instituições democráticas. Assim, o caso serve como um alerta para a urgência de aprimorar o arcabouço normativo brasileiro, especialmente no que se refere à proteção dos usuários frente ao poder das plataformas digitais (Zuboff, 2019; Silva, 2024; Cassino; Souza; Silveira, 2021).

Esse episódio serve, portanto, como ponto de inflexão para a compreensão de um fenômeno mais amplo e estrutural: o colonialismo de dados. Ao transpor a lógica de apropriação e controle de recursos para o ambiente digital, as *big techs* consolidam novas formas de dominação e dependência, aprofundando desigualdades e colocando em xeque a

soberania informacional de países e populações inteiras (Cassino; Souza; Silveira, 2021; Zuboff, 2019).

Diante desse cenário, o caso Cambridge Analytica reafirma a centralidade do debate sobre proteção de dados e soberania informacional, destacando a necessidade de políticas públicas e regulações que garantam não apenas a proteção individual, mas também a autonomia coletiva frente ao poder das grandes corporações digitais (Cassino; Souza; Silveira, 2021; Zuboff, 2019).

Diante disso, é possível extrair algumas lições relevantes à luz dos fundamentos jurídicos e teóricos desta pesquisa. A análise do caso Cambridge Analytica revela, de forma paradigmática, as limitações do consentimento como fundamento legítimo para o tratamento de dados pessoais em plataformas digitais. Ainda que os usuários tenham formalmente autorizado o uso de suas informações, o contexto técnico assimétrico e a opacidade dos mecanismos de coleta impediram uma compreensão plena sobre os reais fins do tratamento.

Tal episódio reforça a tese de que a autodeterminação informativa e o livre desenvolvimento da personalidade não podem ser efetivamente garantidos por modelos de autorregulação centrados exclusivamente na vontade individual. Além disso, ao capturar e explorar traços comportamentais para manipulação política, a prática de *profiling* interfere diretamente na construção da identidade, violando sua autonomia subjetiva e reconfigurando seus percursos identitários.

O escândalo expôs, assim, a necessidade de estruturas regulatórias robustas, capazes de impor limites ao uso massivo e opaco de dados pessoais e de assegurar, de fato, a soberania informacional dos usuários. Nesse sentido, o caso serve como alerta para o ordenamento jurídico brasileiro, especialmente quanto à interpretação e aplicação dos princípios da LGPD diante de um ambiente de constante datificação.

5.2 Colonialismo de dados e o monopólio GAFAM

A ideia desta pesquisa é estudar o instituto da perfilização à luz do direito fundamental do livre desenvolvimento. Entretanto o trabalho visa posicionar a perfilização como parte de uma engrenagem maior, o capitalismo de vigilância, com suas implicações sob o direito do livre desenvolvimento. Conforme já abordado por este trabalho, tal qual o capitalismo tradicional, o capitalismo de vigilância concentra seu poder, agora instrumentário, em um pequeno grupo de big techs.

Neste item a pesquisa visa apresentar os atores desta nova forma de colonialismo, qual seja, o anacrônico GAFAM, formado por: Google, Apple, Facebook, Amazon e Microsoft. Utilizaremos o conceito de colonialismo digital do especialista em cibersegurança e estudioso do assunto, Rodolfo Avelino, que define o instituto como:

O colonialismo digital consiste na prática de aprisionamento tecnológico no ecossistema digital de dispositivos eletrônicos, protocolos de rede, linguagens de máquina e programação. Esse ecossistema é a via que permite a internet realizar a comunicação, a transferência e o processamento de dados pessoais, sistemas e serviços (Avelino, 2021, p. 73).

O capitalismo e o colonialismo mantêm uma relação estrutural e histórica de interdependência. O colonialismo operou como mecanismo de expansão do capitalismo, proporcionando acesso a recursos naturais, mão de obra barata e novos mercados para as metrópoles europeias. O colonialismo não foi um estágio pré- capitalista, mas uma ferramenta ativa de sustentação do capitalismo, garantindo fluxo contínuo de excedentes das colônias para as economias centrais (Avelino, 2021).

O colonialismo de dados emerge como um paradigma contemporâneo, transpondo a lógica colonial para o âmbito digital cujo pilares são:

- **Apropriação de recursos intangíveis:** Dados pessoais substituem recursos naturais como matéria-prima, extraídos massivamente por corporações e Estados.
- **Infraestrutura de extração:** Plataformas digitais e algoritmos atuam como "novos territórios colonizados", onde interações humanas são monitoradas, quantificadas e mercantilizadas.
- **Hierarquias reprodutoras de poder:** Assim como o colonialismo histórico criou divisões raciais, o colonialismo de dados gera assimetrias entre detentores de tecnologia (EUA, China) e populações "datificadas".

Ocorre que neste novo modo de apropriação, ao invés de territórios físicos as grandes empresas buscam colonizar territórios digitais, e com o monopólio dessas tecnologias tais empresas conseguem explorar territórios em todo o mundo, porém concentrando poder e recursos em um único país, os Estados Unidos (Avelino, 2021, p. 74).

Países como a China e Coreia do Sul tem se atentado para a importância dos dados como recurso político de soberania e autonomia tecnológica, passando a investir internamente em políticas de soberania digital e restringindo o acesso de adversários a tecnologias

sensíveis. A China, por exemplo, tem se destacado no avanço de tecnologias de Inteligência artificial, liderando por exemplo em áreas estratégicas de tecnologias como criptomoedas, pequenos drones, comércio eletrônico, fabricação de dispositivos móveis, reconhecimento facial (Accioly Filho, 2025).

Todavia, a tentativa de romper com a dependência tecnológica em relação aos EUA tem gerado tensões políticas e econômicas entre os países. Os EUA tentam frear a ascensão tecnológica chinesa através de barreiras tarifárias à indústria chinesa, que por sua vez responde com restrições à exportação de minérios críticos necessários à cadeia de produção. Alguns estudos inclusive já consideram que no que tange a digitalização, não se pode mais falar em um único polo de concentração de poder, mas sim dois, compostos por China e EUA. Contudo não adentraremos nesta discussão, limitando a discutir apenas o acúmulo das empresas norte americanas, que dominaram o mercado com exclusividade nas últimas décadas (Avelino, 2021, p. 76)

A partir da Cúpula Mundial da Sociedade da Informação de 2005, evento que reuniu governos, entidades empresariais e sociedade civil para discutir aspectos técnicos, políticos e sociais da rede mundial de computadores, verificou-se, com base na teoria do professor de direito Yochai Benkler que a rede de computadores opera com base em três camadas: (i) Infraestrutura das telecomunicações; (ii) Padrões e serviços técnicos da internet; (iii) Padrões de conteúdos e aplicativos.

Em cada uma dessas camadas é possível se extrair dados e metadados utilizados como diferenciais competitivos na economia informacional, onde as big techs mencionadas neste item têm se posicionado de forma incisiva em pontos estratégicos desta infraestrutura (Avelino, 2021, p.80).

Iniciando pela infraestrutura física, que garante a comunicação entre países e continentes, que por muitos anos eram gerenciados quase que exclusivamente por empresas de telecomunicações. Entretanto, no Brasil, a Google e o Facebook instalaram cabos ópticos na faixa litorânea de estados mais estratégicos do país (Cassino, Souza, Silveira, 2021).

O Facebook, com infraestrutura de dados no Rio de Janeiro e Praia Grande, litoral de São Paulo e o Google em Fortaleza, Santos e Rio de Janeiro, além de mais de 90 pontos de internet e mais de 100 instalações de interconexão em todo o mundo. A Amazon também vem se posicionando na prestação de serviços de provedor de internet através do projeto Kuiper, que oferece internet residencial via satélite, com planejamento de implantar um total de 3.236 satélites para expandir o acesso global à internet.

Ao construir infraestruturas próprias, empresas como a Meta buscam garantir desempenho e segurança para seus serviços, mas também consolidam uma posição privilegiada no tratamento do tráfego de dados. No entanto, essa estratégia colide com o princípio da neutralidade da rede, consagrado no Artigo 9º do Marco Civil da Internet brasileiro, que exige o tratamento isonômico de todos os pacotes de dados, independentemente de origem, destino ou serviço. Projetos similares como o *Free Basics*, foram banidos na Índia por violar o princípio da neutralidade da rede.

No Brasil, o *Free Basics* foi anunciado como uma alternativa para ampliar o acesso à internet em regiões com baixa conectividade, especialmente no Norte do país, onde o custo do acesso ainda é uma barreira significativa para grande parte da população. No entanto, ao contrário da Índia, o *Free Basics* não foi proibido no Brasil, embora tenha enfrentado resistência e debate quanto à sua adequação ao Marco Civil da Internet e à legislação nacional sobre neutralidade da rede.

Apesar da ausência de uma proibição formal, como ocorreu na Índia, o projeto não prosperou no Brasil devido à pressão regulatória, ao debate público sobre a limitação de conteúdos e ao receio de favorecer monopólios digitais. Vale lembrar que, caso o Facebook/Meta passasse a oferecer diretamente um serviço de acesso à internet, estaria acumulando, para fins do Marco Civil da Internet, as funções de provedor de conexão, normalmente exercida por operadoras de telecomunicações, e de provedor de aplicações de internet, como já atua por meio das redes sociais que administra.

Essa sobreposição funcional, embora não expressamente vedada, poderia acarretar riscos regulatórios, uma vez que contraria a lógica da separação de papéis, podendo comprometer princípios como a neutralidade da rede e acentuar práticas anticoncorrenciais por meio da priorização de seus próprios serviços.⁴¹.

A neutralidade da rede é um princípio fundamental para garantir que todos os dados na internet sejam tratados de forma igualitária, independentemente de sua origem, destino, conteúdo ou aplicação. Isso significa que provedores de internet não podem bloquear, acelerar ou desacelerar o acesso a determinados sites ou serviços, nem criar “vias rápidas” para empresas que possam pagar por esse privilégio. A neutralidade da rede visa proteger a

⁴¹ Art. 5º Para os efeitos desta Lei, considera-se:

V - Conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;

VII - Aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet;

liberdade de expressão, promover a inovação e garantir a livre concorrência, evitando que grandes empresas monopolizem o acesso à informação e limitem o surgimento de novos negócios e ideias online.

Nesse contexto, é importante observar que o domínio das *big techs* não se limita à infraestrutura de rede, mas se estende também ao controle sobre *softwares* essenciais e serviços estratégicos, impactando diretamente outros setores-chave do ecossistema digital (Avelino, 2021). A Microsoft, por exemplo, lidera o segmento de suítes de escritório, monopolizando as máquinas com seu sistema operacional e aplicativos de escritório, Office (Avelino, 2021, p. 76).

Migrando para a parte de educação, em 2020 o grupo de pesquisa intitulado Observatório Educação Vigiada, realizou um estudo de mapeamento da relação das instituições públicas brasileiras de educação com os serviços ofertados de tecnologia ofertado pelas grandes empresas estrangeiras. O estudo teve como objeto o capitalismo de vigilância nas instituições de nível superior e demonstrou que todas as universidades federais brasileiras possuem vínculo com as gigantes do vale do silício e 44 das 68 instituições possuem contrato com as empresas do GAFAM, em especial Google e/ou Microsoft (Cruz; Saraiva; Amiel, 2019; Mian, 2021, p. 126).

Esse movimento de concentração de poder evidência como as *big techs* expandem sua influência para além da infraestrutura básica da internet, consolidando posições dominantes também no fornecimento de softwares e soluções digitais indispensáveis ao funcionamento de instituições públicas e privadas. O controle sobre sistemas operacionais, suítes de escritório e plataformas educacionais reforça a dependência tecnológica e amplia o alcance dessas corporações sobre dados sensíveis e estratégicos, criando desafios para a autonomia nacional e a proteção de dados no ambiente digital (Avelino, 2021; Cruz; Saraiva; Amiel, 2019; Mian, 2021).

A partir dos números encontrados, o Observatório Educação Vigiada tece a crítica sobre a relação de assimetria informacional e o potencial de violação de privacidade, visto que os *softwares* são disponibilizados de forma gratuita, em troca da coleta, tratamento, utilização e comercialização dos dados comportamentais dos usuários, incluindo aqui alunos e professores, além dos dados de pesquisa institucional e a própria comunicação interna das instituições (Cruz; Saraiva; Amiel, 2019; Observatório Educação Vigiada, [2025]).

Ao terceirizarem serviços essenciais para empresas estrangeiras, as instituições de ensino superior expõem não apenas dados acadêmicos, mas também informações sensíveis de

toda a comunidade universitária, ampliando os riscos de exploração econômica e de perda de autonomia sobre o conhecimento produzido localmente. Essa lógica de dependência tecnológica e exploração de dados não se limita ao setor educacional, mas se estende de maneira transversal a outros campos estratégicos, como a saúde, (Cruz; Saraiva; Amiel, 2019; Avelino, 2021)

Mariella Batarra Mian (2021, p. 136), doutoranda e mestra em ciências Humanas e Sociais pela universidade federal do ABC, aborda o tema em seu artigo , *Universidades Federais Brasileiras a serviço da Lógica Colonial de Exploração de Dados* e ressalta os cortes orçamentários a partir de 2016 como um dos motivos que colaboram para o aceite das universidades em contratar estes serviços, visto que não há necessidade de remuneração direta, que em tese geraria uma economia à instituição.

Entretanto, Mian (2021, p. 136) analisa que em tempos de capitalismo de vigilância e colonialismo de dados a adesão a esta prática pode causar exatamente o efeito contrário ao desejado, pelo que chamou de *mito do custo-benefício* pois, na prática, as instituições se tornam locais de exploração pelas *big techs* GAFAM, gerando informações de alto valor a um baixo custo.

Já a jornalista e cientista social Joyce Souza (2021) analisou o colonialismo de dados no contexto da saúde brasileira, em especial para fins de treinamento de ferramentais de IA no período pós pandêmico. A autora observou que aumentaram as iniciativas estatais que possibilitassem atendimento, acompanhamento e marcação de consultas online, garantindo o distanciamento social necessário à época. Contudo, ao analisar os portais do Ministério da Saúde e das secretarias de saúde de estados e municípios, apontou que não há informações consolidadas sobre como tais aplicativos operam, seus atores e as finalidades específicas de cada um.

Souza traz o alerta sobre o valor dos dados de saúde e as possibilidades da perfilização de perfiz de saúde para fins discriminatórios que já têm sido praticadas. Nas palavras da autora:

Nos Estados Unidos, por exemplo, empresas estavam reunindo milhões de registros de receitas farmacêuticas e vendendo-as para as seguradoras responsáveis pela comercialização de planos de saúde. Com essas informações em posse, as seguradoras tinham "a opção de escolher a cereja saudável em vez do limão doente" e ter muito mais lucro do que aquelas que aceitavam a todos (Souza, 2021, p. 117).

Por fim, é importante ressaltar que embora o capitalismo de vigilância, o capitalismo de plataforma, o colonialismo de dados e o colonialismo digital tenham como foco principal ativos imateriais, sua existência depende de uma robusta infraestrutura física. Não há *software* sem *hardware*: *data centers*, cabos ópticos e dispositivos conectados exigem grande consumo energético e recursos naturais, o que perpetua a dependência dos países periféricos como fornecedores de matéria-prima, mão de obra e, muitas vezes, como destinos de resíduos tóxicos, conforme apontam Cassino, Souza e Silveira (2021) e Avelino (2021).

Essa dinâmica reforça a posição vulnerável dessas nações no cenário global, agravando desigualdades e comprometendo, inclusive, o livre desenvolvimento da personalidade e a autodeterminação informativa de suas populações. Ainda que não se aprofunde aqui nos impactos ambientais e sociais do desenvolvimento tecnológico, é fundamental reconhecer que tais efeitos colaterais estão intrinsecamente ligados ao debate sobre colonialismo de dados e merecem atenção em futuras discussões e formulações regulatórias Cassino, Souza e Silveira (2021).

5.3 Harmonização jurídica internacional, soberania digital e desafios globais da proteção de dados

Este item tem como objetivo analisar as dificuldades e os caminhos para a harmonização jurídica internacional diante da crescente circulação de dados e a atuação transnacional das grandes plataformas digitais, que colocam à prova a capacidade da legislação de atender aos múltiplos interesses e se adaptar a um cenário que está em desenvolvimento constante e transformações que ocorrem em uma velocidade nunca antes vista.

O fluxo internacional de dados não é uma preocupação apenas do Estado brasileiro, discutido pela União Europeia no caso popularmente conhecido como “Schrems II” (caso C-311/18), que questionou o modelo de compartilhamento de dados internacionais. O caso também foi motivado após o episódio de espionagem internacional revelado por Edward Snowden em 2013 (Teófilo; Cabella, 2020).

A reclamação de Schrems foi direcionada ao Facebook, que estava transferindo dados pessoais de titulares da União Europeia para os EUA. A reclamação chegou à Suprema Corte Irlandesa e posteriormente, à Cortede Justiça da União Europeia (CJEU), que decidiu que a proteção do *Safe Harbour*, (acordo, estabelecido em 2000 entre os Estados Unidos e a União

Europeia para permitir a transferência de dados pessoais de cidadãos europeus para empresas norte-americanas), era insuficiente para garantir proteção aos dados pessoais transferidos da UE para os EUA (Teófilo; Cabella, 2020).

A União Europeia entendeu que o programa de espionagem implantado pelo governo norte-americano representou uma violação desproporcional dos direitos relacionados à privacidade e proteção de dados garantidos pela GDPR. Como resposta, a União europeia derrubou o acordo e criou cláusulas padrões para garantir condições mínimas de preservação de direitos no compartilhamento de dados⁴²

A experiência europeia evidencia que a proteção efetiva de dados pessoais em cenários transnacionais exige não apenas normas robustas, mas também mecanismos de fiscalização e revisão contínua, o que serve de referência para o contexto brasileiro.

No Brasil, a transferência internacional é mencionada na Seção 5 da LGPD, que estabelece as hipóteses em que a transferência internacional é permitida, prevendo no art. 33, II, a) e b) a possibilidade de edição de cláusulas contratuais específicas e cláusulas padrão para a transferências, função esta que caberia à ANPD.

No contexto brasileiro, a dependência de serviços e infraestruturas tecnológicas estrangeiras, especialmente das *big techs*, agrava os desafios para a efetiva proteção de dados e soberania digital. A ausência de mecanismos específicos para controlar o fluxo internacional de dados, aliada à centralidade do consentimento como base legal, evidencia a vulnerabilidade dos titulares brasileiros diante de práticas globais de coleta e tratamento de dados, dificultando a garantia dos direitos fundamentais previstos na LGPD (Cassino, Souza, Silveira, 2021. Avelino 2021).

O tópico foi levado em pauta na Tomada de Subsídios realizada pela ANPD em 2022 e em 2024 foi publicada a resolução CD/ANPD nº19/2024 que regulamenta os artigos 33 e 36 da LGPD (Silva et al., 2022; ANPD, 2024).

No contexto brasileiro, a aplicação das novas regras sobre transferência internacional de dados, estabelecidas pela Resolução CD/ANPD nº 19/2024, não ocorre de maneira automática para todas as operações envolvendo redes sociais. A incidência dessas normas depende da análise da natureza jurídica da operação de transferência de dados. De acordo com a regulamentação, apenas as transferências realizadas por controladores ou operadores que

⁴²As cláusulas contratuais padrão consistem em modelos de cláusulas, pré-aprovadas pela Comissão Europeia, que podem ser incluídas nos contratos que envolvem transferência internacional de dados entre União Europeia e outros territórios, como medida de salvaguarda para garantir os padrões mínimos de segurança e proteção aos direitos garantidos pela GDPR e viabilizar o compartilhamento dos dados (Silva et al., 2022).

estejam formalmente estabelecidos no Brasil estão sujeitas aos mecanismos e exigências definidos pela ANPD.

Por outro lado, quando empresas estrangeiras, incluindo redes sociais sediadas fora do país, coletam dados diretamente dos usuários brasileiros, sem a participação de intermediários locais, essa operação não é caracterizada como "transferência internacional" nos termos do artigo 33 da LGPD. Nesses casos, a regulamentação específica da Resolução CD/ANPD nº 19/2024 não se aplica, dispensando a obrigatoriedade de cláusulas contratuais padrão ou outros mecanismos adicionais previstos para transferências internacionais. Assim, tais operações permanecem submetidas apenas às bases legais gerais da LGPD, como o consentimento do titular, sem a necessidade de observância das cláusulas específicas para envio de dados ao exterior (ANPD, 2024; Silva et al., 2022).

Nesses casos, a responsabilidade pelas operações segue vinculada às bases legais gerais da LGPD, sem a necessidade da observação das cláusulas padrões de transferência internacional editadas pela ANPD, mantendo o consentimento como base legal, sem exigência de cláusulas específicas para o envio de dados ao exterior (ANPD, 2024).

Trazendo o posicionamento da ANPD para o objeto da pesquisa, verificou-se um problema sobre à isenção da obrigatoriedade de cláusulas padrão nos casos em que as empresas os façam sem intermediários, em contato direto com os usuários, pois no caso da Meta Platform Inc. a empresa sinaliza aos usuários que os dados serão compartilhados com empresas parceiras, logo, haverá uma transferência à terceiros (que podem ser nacionais ou internacionais). Entretanto, não foi possível identificar se as orientações da ANPD seriam obrigatórias às operações das redes meta. Pelo conjunto de informações dar-se a ideia de que neste caso o consentimento do usuário permanece como a base legal que permite estes compartilhamentos de dados entre as empresas.

Ao consentir com os termos de uso, o titular autoriza o compartilhamento de seus dados com as empresas parceiras e com as demais empresas controladas pelo grupo Meta, que não necessariamente serão de rede social, logo o entendimento de que a rede social faz a captação sem intermediários pode ser relativizado se o grupo agir como um intermediário entre seus diferentes produtos. Neste ponto, de acordo com os itens analisados até o momento, compartilhamos do posicionamento de que o consentimento por si só não é a base legal adequada ao tratamento de dados feitos para fins de perfilização nas redes sociais.

Ao longo desta pesquisa foram apresentadas diversas críticas à prática de perfilização realizada pelas redes sociais da empresa Meta, pontuando desafios de ordem jurídicas, sociais

e regulatórias, que se mostram inexistente e hora se mostram insuficientes à resolução dos problemas apontados. Diante o exposto traremos na Seção 6 algumas iniciativas que têm sido pensadas pela doutrina brasileira como forma de iniciar um debate e fornecer subsídio teórico para soluções futuras, de modo a atender um dos objetivos específicos elencado na introdução deste trabalho.

Fato é que o equilíbrio entre desenvolvimento tecnológico e proteção de direitos fundamentais não é matéria simples de se solucionar, especialmente se analisadas sob uma ótica polarizada em que a defesa de um deva obrigatoriamente implicar na anulação do outro. Por óbvio, diante da complexidade do tema, esta pesquisa não tem a intenção de dizer de forma exaustiva quais soluções devem ser adotadas, mas apontar possíveis caminhos capazes de ponderar tais interesses.

Para tanto, levantamos aqui o que se consideram as principais críticas realizadas, sendo elas: (i) A ineficácia do consentimento como a principal base legal para disciplinar o profiling nas redes sociais da empresa meta; (ii) as lacunas regulatórias da LGPD sobre as decisões automatizadas para fins de perfilização; (iii) O impacto desta prática no livre desenvolvimento da personalidade; (iv) A vulnerabilidade estrutural tecnológica.

Das iniciativas que serão apresentadas, partiremos do pressuposto da necessidade de aplicação dos direitos fundamentais também nas relações privadas, entre particulares, e não apenas de forma vertical entre o estado e indivíduos. Para tanto, traremos a analogia feita pelo professor de Direito constitucional, Daniel Sarmento, que dedica parte de sua obra para tratar do assunto (Bioni, 2019; ANPD, 2024; Sarmento, 2004).

5.4 O devido processo informacional e horizontalidade de direitos fundamentais

Sarmento (2003) analisa a horizontalidade dos direitos fundamentais a partir de sua obra *Direitos fundamentais e Relações privadas*, à época o autor pontua, que a aplicação dos direitos fundamentais entre particulares ainda era vista de maneira controversa, se dividindo entre correntes que negavam a aplicação por completo, e outras que aceitavam tal aplicação de forma irrestrita. Todavia, atualmente pode se afirmar com fundamento na doutrina e na jurisprudência brasileira que, mesmo nas relações entre particulares, os direitos fundamentais garantidos constitucionalmente devem ser observados. Tendo como marco o recurso extraordinário RE 201.819-8, vejamos:

EMENTA: SOCIEDADE CIVIL SEM FINS LUCRATIVOS, UNIÃO BRASILEIRA DE COMPOSITORES. EXCLUSÃO DE SÓCIO SEM GARANTIA DE AMPLA DEFESA E DO CONTRADITÓRIO. EFICÁCIA DOS DIREITOS FUNDAMENTAIS. RECURSO DESPROVIDO. I. EFICÁCIA DOS DIREITOS FUNDAMENTAIS NAS RELAÇÕES PRIVADAS. As violações aos direitos fundamentais não ocorrem somente no âmbito das relações entre cidadão e o estado, mas igualmente nas relações travadas entre pessoas físicas e jurídicas de direito privado. Assim, os direitos fundamentais assegurados pela constituição vinculam não apenas os poderes públicos, estando direcionados também à proteção dos particulares em face dos poderes privados (Brasil, STF, RE 201.819-8, 2005).

O julgado se faz relevante, pois além de reconhecer a eficácia horizontal dos direitos fundamentais entre particulares, firmando tal precedente jurisprudencial, aborda a necessidade de um devido processo legal no âmbito administrativo, reforçando a necessidade de contraditório e ampla defesa também em processos administrativos entre pessoas jurídicas de direito privado e particulares (Brasil, STF, RE 201.819-8, 2005).

Avançando na análise jurídica, temos também o julgamento da Ação Direta de Inconstitucionalidade, conhecida como caso IBGE, que foi objeto de estudos na Seção 3, que aplica entendimento ao contexto da proteção de dados no contexto de tomada de decisões automatizadas que afetem as liberdades individuais, o que tem sido chamado de *devido processo informacional*, instituto o qual entendemos que se aplica ao objeto desta pesquisa.

Como já mencionado ao longo do trabalho, a opacidade das relações, em especial sobre o funcionamento dos algoritmos, pode gerar perfilamentos equivocados e discriminatórios, de forma a refletir, negativamente, no livre desenvolvimento da personalidade dos usuários, tanto na percepção de si como na percepção do outro, como exposto no item 3.4.2 *profiling* e identidade, a partir do referencial teórico de Ricoeur da identidade narrativa, e ilustrado a partir do caso do COMPAS.

Pelo conjunto de normas, atualmente endossadas pela doutrina e jurisprudência brasileira, pode se chegar à conclusão, que a garantia do devido processo informacional não deve se limitar às relações entre Estado e particulares, alcançando assim outras formas de relações se necessário, a fim de coibir arbitrariedades, seja por parte do estado seja por parte de particulares (Bioni; Martins, 2020).

A prática de perfilização gera uma expressiva desigualdade de poder entre quem é perfilado e quem realiza o perfilamento. O sujeito acaba por perder a capacidade de definir sua própria identidade e de influenciar a interpretação de suas ações, o que compromete sua autonomia.

quanto maior for a desigualdade, mais intensa será a proteção ao direito fundamental em jogo, e menor a tutela da autonomia privada. Ao inverso, numa situação de tendencial igualdade entre as partes, a autonomia privada vai receber uma proteção mais intensa, abrindo espaço para restrições mais profundas ao direito fundamental com ela em conflito (Sarmento, 2004, p. 303).

Poucas relações entre entidades privadas podem se dar de forma mais desigual do que entre um titular de dados e um controlador de dados que se utiliza técnicas de profiling para avaliar e prever seus comportamentos. Portanto, há de se reconhecer a eficácia horizontal da garantia constitucional do devido processo (Citron, Pasquale. 2014, p. 19)

Importante ressaltar que, como já dito no início do item, o que se propõe como solução é um diálogo de interesses, de modo que o devido processo informacional não seja visto como um freio ao desenvolvimento tecnológico, fazendo incidir um excesso de proceduralização, mas apenas um meio para a finalidade, que é uma ponderação justa de interesses.

O perigo da excessiva proceduralização, foi pontuado inclusive pela própria ANPD, que reconheceu que a exigências de forma individual e pormenorizada, seria tecnicamente impraticável, e até indesejável para a proteção de direitos se observado por uma perspectiva de uma política pública (ANPD, 2025).

Assim, sustentamos que o devido processo informacional deve funcionar como um parâmetro normativo para a realização de atividades automatizadas de tratamento de dados, especialmente quando essas possam impactar os interesses e direitos fundamentais dos titulares dos dados.

6 INICIATIVAS DE REEQUILÍBRIO DE INTERESSES

Como alternativa para promover o devido processo informacional, incorporamos à análise o conceito de “direito a inferências razoáveis”, proposto por Wachter e Mittelstadt (2019). Embora ainda seja um conceito jurídico indeterminado e em fase de maturação, ele oferece um ponto de partida promissor para repensar o equilíbrio entre inovação tecnológica e direitos fundamentais.

6.1 Direito a Inferências Razoáveis

Conforme discutido nas seções anteriores, a predição de comportamentos e a formulação de inferências, especialmente aquelas obtidas por sistemas automatizados, interferem diretamente na autonomia do sujeito de se auto narrar. Contudo, defendemos neste trabalho que a disputa pela formação dessa identidade não representa um problema em si, já que de acordo com a teoria adotada, as narrativas externas se tornam parte das dinâmicas de interação social, logo, o indivíduo recebe atribuições identitárias de outros agentes, que podem ou não aceitar a identidade que ele mesmo reivindica.

No entanto, o que se questiona é a possibilidade de que essa disputa narrativa ocorra de forma justa, permitindo ao indivíduo a possibilidade de participar da desta construção e interagir com as narrativas externas, incluindo as realizadas por decisões automatizadas para fins de perfilização.

No contexto das redes sociais, tais características identitárias são deduzidas com base em dados observáveis, partindo de informações que não necessariamente são informadas pelos usuários, a exemplo das curtidas no qual se infere o gosto dos usuários por determinados assuntos, sem que este tenha confirmado tais interesses, o que compromete a autonomia informacional do indivíduo e dificultando sua capacidade de contestar ou compreender os critérios utilizados, visto que se quer tem consciência de todos os dados a respeito de si que estão sendo tratados.

Wachter e Mittelstadt (2019) propõem, portanto, o reconhecimento de um “direito a inferências razoáveis” como mecanismo de proteção de dados. Tal direito implicaria impor aos controladores de dados o ônus de justificar que as inferências automatizadas são geradas com base em critérios razoáveis. Segundo os autores, isso significaria exigir:

(i) uma justificativa ex ante demonstrando por que determinados dados são uma base normativamente aceitável para extrair inferências; (ii) a demonstração de que essas inferências são relevantes e normativamente aceitáveis para os fins de tratamento de dados ou decisões automatizadas específicas; (iii) a comprovação de que os dados e métodos utilizados são estatisticamente confiáveis e precisos (Wachter; Mittelstadt, 2019, p. 19, tradução nossa).

Essas exigências devem se aplicar, sobretudo, nos casos em que são extraídas “inferências de alto risco”. Os autores propõem dois critérios alternativos para identificá-las: (i) inferências que apresentam ameaça ou risco significativo à reputação ou privacidade dos titulares; e (ii) inferências cuja precisão não pode ser verificada adequadamente, mas que ainda assim servem de base para decisões com efeitos relevantes sobre os indivíduos, nas palavras dos autores:

Nos casos em que os algoritmos extraem “inferências de alto risco” sobre indivíduos, esse direito exigiria que o controlador de dados fornecesse uma justificativa ex ante para estabelecer que a inferência a ser extraída é razoável. Essa divulgação abordaria (1) por que certos dados formam uma base normativamente aceitável a partir da qual extrair inferências; (2) por que essas inferências são relevantes e normativamente aceitáveis para o objetivo de processamento escolhido ou o tipo de decisão automatizada; e (3) se os dados e métodos utilizados para extrair as inferências são precisos e estatisticamente confiáveis. Esses requisitos devem ser impostos por meio da introdução de requisitos de verificação e notificação legalmente vinculantes a serem atendidos pelos controladores de dados antes da implantação em escala de análises inferenciais de alto risco. (Wachter, Mittelstadt, 2019, tradução nossa).

No contexto das redes sociais, entendemos que ambas as hipóteses são aplicáveis. No entanto, reconhecendo as limitações técnicas de uma revisão individualizada em larga escala, propomos, como complemento à proposta dos autores, a inclusão de um mecanismo regulatório institucionalizado, conforme segue:

(i) Participação da Autoridade Nacional de Proteção de Dados (ANPD) como terceiro interessado, com competência para definir parâmetros objetivos do que constitui uma inferência razoável. A atuação da ANPD poderia se iniciar pela distinção entre dados necessários à funcionalidade e otimização do serviço e aqueles excedentes, o chamado *superavit comportamental*, já abordado pelo trabalho em item próprio.

Esta proposta está em consonância com o art. 55-J da LGPD, que atribui à ANPD a competência para regulamentar matérias relacionadas à proteção de dados, inclusive no que diz respeito ao uso ético e proporcional da inteligência artificial. Um paralelo pode ser traçado com autoridades como o CNIL, na França, ou a AEPD, na Espanha, que já exercem papel semelhante no controle preventivo de inferências automatizadas.

A proposta de reconhecimento de um direito a inferências razoáveis também deve ser compreendida como um instrumento de efetivação dos princípios fundamentais previstos no art. 2º da LGPD, notadamente o respeito à autodeterminação informativa (inciso II) e ao livre desenvolvimento da personalidade (inciso III). Ao limitar as inferências a critérios de razoabilidade, precisão e relevância, estabelece-se um filtro normativo que impede o tratamento excessivo, opaco ou discriminatório, permitindo que os indivíduos não sejam reduzidos a perfis ou classificações automatizadas desprovidas de contexto ou controle.

Ademais, a vinculação da inferência razoável aos princípios da finalidade e da necessidade (art. 6º, incisos I e II), reforça o dever das plataformas de justificar *ex ante* (anterior) a coleta e utilização de dados, especialmente quando o tratamento se destina à segmentação comportamental para fins econômicos. O “direito a inferências razoáveis” surge, assim, como um instrumento de densificação dos princípios da LGPD, funcionando como uma ponte normativa entre os fundamentos constitucionais da proteção de dados e a realidade tecnológica das plataformas digitais.

Além disso, o reconhecimento do direito a inferências razoáveis se apoiaria em três critérios operacionais consagrados pela doutrina brasileira: finalidade legítima, necessidade e proporcionalidade. Esse tripé normativo permitiria que as inferências fossem possíveis tecnicamente, entretanto necessitariam ser juridicamente justificadas. Assim haveria a segurança de um terceiro tecnicamente capaz mediando os interesses entre plataforma e usuários, um equilíbrio entre os direitos fundamentais e o avanço tecnológico. Assim não seria necessário que cada usuário precisasse intervir pessoalmente, evitando um excesso de proceduralização, que poderia tornar o mecanismo tecnicamente inviável.

Vale lembrar que, como ressaltam os próprios autores, há uma lacuna regulatória crítica, lacuna está na qual incluímos aqui a legislação brasileira. Os autores pontuam que a legislação atual tende a proteger apenas as decisões tomadas com base nos dados, mas não o processo inferencial anterior a elas. Essa omissão se faz problemática, pois muitas das decisões mais invasivas não são formalmente “automatizadas” ou decisórias, mas decorrem

de inferências classificatórias e probabilísticas que escapam da regulação tradicional (Wachter; Mittelstadt, 2019).

Ademais, a proposta busca enfrentar a chamada opacidade algorítmica, na qual os indivíduos não conseguem compreender ou verificar como foram classificados ou rotulados. Ao transferir para os controladores o ônus de provar a razoabilidade das inferências, o direito proposto pretende restaurar certa simetria entre os sujeitos dos dados e as redes sociais.

Em conclusão, o reconhecimento de um direito a inferências razoáveis não representa uma barreira à inovação. Pelo contrário, cria um ambiente de previsibilidade e legitimidade, em que o uso de dados para fins comerciais, como a publicidade comportamental, possa coexistir com a proteção da dignidade informacional dos titulares. A proposta não impede o uso de inferências, mas impõe limites normativos, exigindo que sejam justificáveis, proporcionais e auditáveis.

6.2 Transparência na era do *profiling*: o papel dos relatórios de impacto.

O avanço das técnicas de tratamento automatizado de dados pessoais, como o *profiling* adotado pelas redes sociais da Meta Platforms Inc., tem provocado impactos significativos não apenas na esfera individual, mas também na coletividade. A opacidade desses sistemas algorítmicos, aliada à assimetria técnica e informacional entre usuários e plataformas, dificulta o controle efetivo sobre o uso dos dados e seus efeitos sobre o livre desenvolvimento da personalidade e a autodeterminação informativa, direitos centrais previstos no art. 2º da Lei Geral de Proteção de Dados (LGPD).

Neste contexto, a análise de impacto algorítmico emerge como um importante instrumento jurídico-regulatório para possibilitar o escrutínio público de práticas complexas como a perfilização. Previsto de forma incipiente no art. 38 da LGPD, o relatório de impacto à proteção de dados pessoais (RIPD) busca justamente antecipar os riscos e mitigar danos potenciais relacionados ao tratamento de dados sensíveis ou de alto risco. No entanto, como destaca Bioni (2019, p. 121), a ausência de regulamentação específica e a falta de exigência pública de sua divulgação limitam severamente a eficácia desse dispositivo em contextos de larga escala como o da Meta Inc.

Em sistemas opacos, como os algoritmos de personalização e direcionamento da Meta, não basta a existência de um relatório de impacto interno. É necessário que haja mecanismos externos de controle, como a obrigatoriedade de auditoria independente e a publicização de

informações mínimas para que o titular possa exercer seu direito à autodeterminação informativa. A ausência de transparência sobre os critérios de perfilização, as categorias sensíveis inferidas e os efeitos previsíveis sobre os usuários, compromete o exercício pleno dos direitos previstos nos artigos 6º e 20 da LGPD (Brasil, 2018).

A crítica feita por Doneda (2006, p. 26) à lógica individualista da proteção de dados torna-se ainda mais relevante nesse cenário. Segundo o autor, a proteção da privacidade não pode ser compreendida apenas como uma esfera de escolha individual, exigindo-se abordagens coletivas e mecanismos estruturais de proteção. Mendes (2014, p. 583) complementa que o processamento automatizado de dados pessoais gera externalidades difusas e por isso demanda respostas regulatórias sistêmicas, superando o enfoque exclusivamente contratual do consentimento individual.

Assim, a análise de impacto algorítmico deve ser compreendida não apenas como uma exigência procedural, mas como um instrumento de governança e *accountability*, com potencial de materializar o princípio da responsabilidade previsto no art. 6º, X da LGPD, e permitir o controle democrático sobre tecnologias que moldam o comportamento e a identidade dos indivíduos (Bioni, 2019, p. 145).

O caso da Meta é emblemático nesse sentido. Embora a empresa alegue em seus termos de uso que personaliza a experiência do usuário com base em seus interesses, não há informações claras sobre os limites dessa personalização, tampouco há transparência quanto aos critérios utilizados pelos algoritmos para categorizar perfis ou restringir o acesso aos conteúdos (META, 2025). Tal ausência de clareza viola os princípios da transparência (art. 6º, VI) e da prevenção (art. 6º, VIII), além de dificultar a contestação de decisões automatizadas, conforme previsto no art. 20 da LGPD (Brasil, 2018).

Diante disso, a presente pesquisa defende que o fortalecimento da exigência de análise de impacto, especialmente em contextos de *profiling*, é essencial para garantir a eficácia material da proteção de dados no Brasil. A regulamentação da LGPD deve avançar no sentido de obrigar a realização de RIPDs em toda prática de perfilização com potencial de impactar direitos fundamentais, impondo deveres claros às plataformas digitais. Esses relatórios devem conter, no mínimo, a descrição da lógica envolvida nos algoritmos, as categorias de dados utilizadas, os efeitos previsíveis sobre os titulares, os riscos de discriminação algorítmica e os mecanismos de mitigação adotados (Bioni, 2019, p. 127).

Além disso, o relatório de impacto deve ser vinculado a mecanismos de participação social e controle externo, como defendido por autores que compreendem a proteção de dados

como uma política pública voltada à coletividade (MENDES, 2014, p. 510-512). Esta linha interpretativa é reforçada por abordagens mais recentes que defendem a avaliação de impacto algorítmico como forma de proteção de direitos difusos e promoção da soberania digital (Cassino; Silveira; Souza, 2021).

Assim, a análise de impacto algorítmico não pode ser tratada como mera formalidade documental. No contexto das redes sociais e da economia de dados, trata-se de uma ferramenta necessária para a proteção do indivíduo em sua dimensão coletiva. Sua implementação efetiva é condição indispensável para que a autodeterminação informativa e o livre desenvolvimento da personalidade sejam institutos que se concretizem materialmente, especialmente em face do poder concentrado das *big techs*.

6.3 Iniciativas legislativas e a insuficiência normativa frente à perfilização automatizada

O debate legislativo brasileiro sobre a regulação de plataformas digitais tem avançado de forma fragmentada e silentes aos desafios trazidos pela prática de decisões automatizadas, em especial sobre perfilização no ambiente das redes sociais, como a realizada pela Meta Platforms Inc. Em que pese uma quase ausência de soluções legislativas sobre a perfilização, traremos aqui algumas discussões sobre o tema para fins de contextualizar as iniciativas legislativas, em especial PL 2.630/2020, por entendermos que é o instituto mais próximo do objeto da pesquisa.

6.3.1 Projeto de Lei 2.630/2020 – “PL das Fake News”

O PL 2.630/2020 surge como uma das tentativas mais consolidadas de regular a atuação das grandes plataformas digitais no Brasil. Voltado à transparência na moderação de conteúdo e ao enfrentamento da desinformação, o projeto propõe obrigações como relatórios periódicos sobre políticas de moderação, rastreabilidade de mensagens encaminhadas em massa e identificação de conteúdo patrocinado.

Embora relevante, entendemos que o PL revela limitações importantes quando confrontado com os desafios da perfilização algorítmica baseada em dados pessoais, pois não considerou tal regulação em seu texto. Não há, por exemplo, exigência explícita de divulgação da lógica de funcionamento de sistemas de recomendação, nem previsão de

avaliação de impacto sobre os direitos fundamentais dos usuários, o que, segundo Bioni (2019), é essencial para materializar a responsabilidade no tratamento automatizado.

Ainda que o projeto aponte para uma maior transparência, seu foco está na moderação de conteúdo e não nos processos algorítmicos que organizam e personalizam a experiência digital com base em perfis inferidos. Como argumenta Mendes (2014), a ausência de mecanismos de controle coletivo sobre essas práticas torna a proteção dos direitos informacionais difusa e pouco efetiva.

Dessa forma, embora o PL 2.630/2020 represente um avanço ao reconhecer que as plataformas exercem poder significativo sobre o discurso público, ele não enfrenta a lógica de funcionamento das plataformas enquanto máquinas de extração e exploração de dados pessoais, ponto central da atuação da Meta. A lacuna torna-se ainda mais evidente diante da ausência de obrigação legal para a realização de análise de impacto algorítmico em sistemas que influenciam diretamente o comportamento e a formação da identidade dos usuários.

6.3.2 Projetos sobre inteligência artificial e a omissão sobre perfilização

Nas buscas realizadas foram encontrados três projetos de lei sobre inteligência artificial em tramitação no Congresso Nacional: PL 21/2020, o PL 5051/2019 e o PL 2338/2023. Em tais iniciativas observa-se um esforço de aproximação com as diretrizes internacionais, em especial com o modelo europeu. Contudo, esses textos ainda apresentam abordagem genérica e insuficiente para lidar com práticas específicas como a perfilização automatizada para fins comerciais, especialmente quando realizadas por empresas com posição dominante no mercado.

O PL 2338/2023, por exemplo, classifica sistemas de alto risco com base em seus impactos potenciais, mas não estabelece critérios técnicos claros para identificar práticas de inferência sensível, nem vincula expressamente a necessidade de avaliação de impacto à proteção de dados pessoais. Além disso, nenhum dos projetos menciona a obrigatoriedade de publicização de informações sobre algoritmos de recomendação, nem contempla o princípio da autodeterminação informativa como vetor de interpretação e aplicação normativa – elemento crucial destacado por Doneda (2006) e reafirmado pela LGPD (art. 2º, II).

Conforme aponta Cassino, Silveira e Souza (2021), a ausência de mecanismos que obriguem a transparência e a auditoria independente dos sistemas automatizados favorece a consolidação de um modelo de colonialismo de dados, no qual plataformas transnacionais

extraem valor dos dados de populações periféricas sem qualquer controle democrático. Essa realidade é particularmente preocupante no contexto brasileiro, onde parte significativa da população depende das redes sociais da Meta para acesso à informação, lazer e sociabilidade.

Portanto, embora existam proposições legislativas em curso, elas falham em reconhecer a prática de perfilização na arquitetura das redes sociais e sua capacidade de afetar direitos fundamentais em escala coletiva. A ausência de regulação específica sobre o uso de inferências algorítmicas, somada à inexistência de obrigação legal de análise de impacto, reforça a hipótese desta pesquisa de que, o arcabouço jurídico atual, incluindo a LGPD e os projetos legislativos em andamento, é materialmente insuficiente para proteger a autodeterminação informativa dos usuários frente à lógica de funcionamento da Meta Platforms Inc.

6.4 Reavaliação do Consentimento e Propostas de Solução para o *Profiling* em Redes Sociais

Esta subseção avança no estado da técnica ao discutir a necessidade de uma reavaliação crítica do papel do consentimento como base legal para o tratamento de dados pessoais, especialmente no contexto do *profiling* em redes sociais. A partir das obras de referência, serão apresentadas as principais críticas ao modelo tradicional de consentimento, destacando suas limitações diante da complexidade técnica e da assimetria informacional entre usuários e plataformas digitais.

Em seguida, serão expostas as soluções propostas por Bruno Bioni, que levanta algumas discussões sobre como equilibrar a proteção dos direitos fundamentais com as demandas do desenvolvimento tecnológico. O objetivo é fornecer um panorama fundamentado das alternativas regulatórias capazes de responder às críticas identificadas no trabalho, conectando-as diretamente ao objeto da pesquisa: a compatibilidade da prática de perfilização com o livre desenvolvimento da personalidade e a autodeterminação informativa.

Bruno Bioni (2019) destaca que o consentimento, embora central na legislação brasileira, é insuficiente para garantir proteção efetiva em face da complexidade dos sistemas digitais e da incapacidade dos usuários de compreender plenamente os riscos envolvidos no tratamento de seus dados. Para Bioni, o consentimento, como o legítimo interesse, desde que observados os direitos fundamentais e a proporcionalidade.

A partir do referencial teórico da privacidade contextual, proposto por Helen Nissenbaum, Bioni (2019) apresenta uma divisão dos elementos que compõem essa teoria, classificando-os como internos e externos. Antes, porém, de adentrar na análise específica de Bioni, é necessário explicar a lógica da privacidade contextual e situá-la dentro do objeto desta pesquisa.

Segundo Nissenbaum, o trânsito de informações pessoais possui valor social, guiado por considerações políticas e morais. O direito de revelar ou não determinada informação é apenas uma dimensão da privacidade, que não pode ignorar a função social do fluxo de dados. Assim, a análise deve sempre considerar o contexto no qual a coleta e o uso das informações ocorrem, de modo que sejam necessários e socialmente adequados à relação estabelecida (Bioni, 2019).

O uso apropriado, ou não, de uma informação dependerá do contexto em que ela circula. A partir de uma análise heurística da trajetória da informação, estabelece-se a chamada *linguagem informacional*, capaz de indicar se, naquele contexto, o tratamento está ocorrendo de forma íntegra. A soma de integridade e contexto forma o que Nissenbaum denomina, *privacidade como integridade contextual*, sendo o próprio contexto social o responsável por restringir, ou permitir, o fluxo de dados (Bioni, 2019).

A título de exemplo de contextos sociais e tráfego de informações Bioni traz as relações entre médicos e pacientes, pais e filhos. Empregador e empregado, entendendo que cada um destes contextos configura uma esfera social, que geralmente não se comunicam. Não é razoável por exemplo que as informações trocadas entre médico e paciente sejam enviadas ao empregador do paciente, ou que as tocas obtidas no seio familiar sejam compartilhadas com o empregador do indivíduo (Bioni, 2019).

Quanto ao fluxo informacional, o caminho percorrido pela informação entre os atores de um determinado contexto, considera-se interno aquele que permanece na mesma esfera social, conforme os exemplos anteriores. O fluxo interno é natural e necessário ao desenvolvimento da personalidade. Na perspectiva da privacidade contextual, o problema, surge quando há transferência de informações entre esferas distintas, permitindo que um terceiro, estranho à relação originária, interfira. Neste trabalho, esse terceiro será entendido analogicamente pela figura do algoritmo.

Um exemplo concreto dessa interferência de um “terceiro” no fluxo informacional é o experimento conduzido por Kramer, Guillory e Hancock (2014), no qual o *feed* de notícias de aproximadamente 700 mil usuários do Facebook foi manipulado para avaliar se a exposição a

conteúdos predominantemente positivos ou negativos influenciaria o humor expresso por eles. A autorização para essa intervenção foi presumida a partir da aceitação genérica dos termos de uso da plataforma, sem consentimento específico para tal manipulação.

O episódio gerou intenso debate ético e jurídico, revelando que, mesmo em conformidade formal com os termos contratuais, intervenções dessa natureza podem afetar diretamente a experiência e o comportamento do usuário, reforçando a crítica de que o consentimento, isoladamente, não é capaz de garantir a autodeterminação informativa e a integridade contextual (Kramer; Guillory; Hancock, 2014).

Os atores então são o usuário e o conteúdo com o qual este interage, entretanto, o contexto dentro das redes sociais não é necessariamente sabido, podendo ser religioso, profissional, amoroso, e todas as informações são registradas pelo “terceiro ator”/ algoritmo, da mesma forma, logo, diferentemente das esferas sociais tradicionais, no ambiente das redes a esfera social pode ser variável, o que chamaremos aqui de *esfera social fluida*⁴³.

Bioni ressalta que a privacidade serve para proteger os indivíduos de pressões sociais desproporcionais, capazes de comprometer o livre desenvolvimento da personalidade. Nesse sentido, deve ser entendida como um bem comum, indispensável à manutenção de um Estado democrático de direito. Sua proteção, portanto, não beneficia apenas o indivíduo, mas toda a coletividade. É nesse ponto que esta pesquisa se debruça para avançar no estado da técnica e propor uma maior participação estatal, que não elimine o papel do consentimento, mas estabeleça limites ao seu alcance.

Como solução, propõe-se um acompanhamento mais efetivo do Estado nas relações entre usuários e plataformas de redes sociais. Considerando que os efeitos do tratamento de dados são também coletivos, não é razoável que a legitimidade, o interesse e a função social do fluxo de informações pessoais sejam avaliados apenas pelo titular no momento do consentimento. Essa avaliação deve anteceder a coleta e ser realizada por órgão tecnicamente qualificado, como a ANPD. Somente após esse crivo regulatório a plataforma deveria obter o consentimento individual.

Outra limitação que se entende razoável é referente aos dados pessoais sensíveis, quais sejam, aqueles de origem racial, étnica, convicção religiosa, opinião política, filiação sindical,

⁴³ Será entendida como esfera social fluida a relação estabelecida entre as redes sociais e o usuário. Partindo da premissa que os conteúdos são dinâmicos, e escolhidos pela plataforma e que em tese o usuário não tem domínio sobre o conteúdo que terá contato tampouco quais dados serão trocados naquele momento, podendo ser por exemplo algo sobre trabalho, o que seria uma relação contextual, ou sobre moda, que seria outra relação contextual. Entretanto é possível que em um curto espaço de tempo o usuário interaja com ambos os conteúdos, modificando o contexto/esfera social. À esta rápida mutabilidade de contexto damos o nome aqui nesta pesquisa de *esfera social fluida*.

entre outros assim definidos pelo artigo 5º da LGPD, de modo que estes dados não fossem utilizados para fins de publicidade comportamental, ainda que com o consentimento, pois em que pese o princípio da autonomia da vontade das partes, a legislação brasileira também pontua no artigo 11 do Cód. Civil a limitação da vontade das partes para fins de reestabelecimento da ordem pública e reequilíbrio contratual.

Como meio procedural de intervenção do estado, a fim de trazer, mesmo que sem esgotar o tema, traremos aqui algumas as soluções apontadas por Bioni (2019), para a redução da assimetria entre usuários e plataforma a partir da implementação de mecanismos que aumentem a transparência e a participação do titular, como mensagens explicativas claras, sistemas de dupla verificação relatórios de impacto DPIA (*Data Protection Impact Assessment*)⁴⁴ que evidenciem os riscos e as medidas mitigadoras adotadas. promovendo um consentimento mais consciente e um controle mais efetivo do usuário sobre seus dados (Bioni, 2019, p. 140-203).

A implementação de relatórios de impacto à proteção de dados (Data Protection Impact Assessment – DPIA) para operações de *profiling* é uma das principais medidas defendidas por Bioni para mitigar riscos e antecipar consequências negativas do tratamento automatizado de dados pessoais. Ao exigir que controladores avaliem previamente os efeitos de suas práticas sobre os direitos fundamentais dos titulares.

O DPIA está previsto no artigo 38 da LGPD ⁴⁵ e promove uma abordagem preventiva e transparente, alinhando-se ao princípio da responsabilidade e à necessidade de demonstrar conformidade com a legislação. Tal mecanismo contribui para a identificação de riscos específicos do *profiling* e para a adoção de salvaguardas proporcionais, fortalecendo a proteção da personalidade e da autodeterminação informativa dos usuários (Bioni, 2019, p. 187-189).

Outro aspecto central é a participação ativa da autoridade reguladora, especialmente da ANPD, na fiscalização e definição de parâmetros objetivos para decisões automatizadas. Bioni (2019, p. 200-201) sustenta que cabe à autoridade estabelecer diretrizes claras sobre o uso de algoritmos e sistemas de perfilização, bem como fiscalizar o cumprimento das normas pelas plataformas digitais para que as práticas de mercado sejam harmonizadas com os

⁴⁴ O DPIA (Data Protection Impact Assessment) é um relatório obrigatório em determinadas operações de tratamento de dados, conforme artigo 38 da LGPD, que avalia, de forma sistemática, os riscos e impactos potenciais de uma atividade sobre os direitos e liberdades dos titulares, propondo medidas para mitigar eventuais danos

⁴⁵ Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

direitos fundamentais e possibilita a adoção de medidas corretivas em casos de abuso, promovendo segurança jurídica e confiança dos titulares no ambiente digital.

Nos termos do artigo 38 caberia à ANPD a função de determinar a elaboração e os termos desses relatórios de impacto e dialoga com a proposta de publicidade das operações. Além da previsão da LGPD a necessidade de relatórios também foi incluída no projeto de lei 2.630/2020/ PL das *Fake News*, demonstrando uma concordância entre as soluções doutrinárias apresentadas e as iniciativas do legislativo neste ponto

Bioni (2019, p. 203-204) defende que as plataformas devem informar de maneira clara e acessível quais dados são utilizados, quais parâmetros orientam a formação de perfis e de que modo essas decisões impactam a experiência e os direitos dos usuários. Essa transparência não apenas fortalece a autodeterminação informativa, mas também permite que os titulares compreendam e avaliem os riscos associados ao tratamento de seus dados, promovendo uma atuação mais consciente e crítica diante das práticas das plataformas.

Por fim, a criação de canais de contestação e revisão de decisões automatizadas para os titulares é vista como indispensável para assegurar o devido processo informacional e a proteção contra erros ou discriminações algorítmicas. Conforme Bioni (2019, p. 203-204), os usuários devem ter o direito de questionar, revisar e obter explicações sobre decisões que os afetem, especialmente quando baseadas em sistemas automatizados de *profiling*. Esses canais fortalecem a participação do titular no processo decisório, promovem a *accountability* das plataformas e contribuem para mitigar potenciais violações ao livre desenvolvimento da personalidade e à autodeterminação informativa.

Danilo Doneda, por sua vez, concorda com Bioni quanto à insuficiência do consentimento isolado, ressaltando a necessidade de uma proteção dinâmica da autodeterminação informativa que transcenda a mera autorização formal. Doneda enfatiza a importância da transparência algorítmica e do direito à explicação das decisões automatizadas, defendendo que os titulares devem ter a possibilidade de contestar e revisar essas decisões. Contudo, o autor apresenta uma abordagem mais centrada na garantia da liberdade individual e na proteção contra abusos, colocando maior ênfase na participação do titular como forma de empoderamento.

Além desses autores, a literatura consultada reforça a necessidade de soluções que integrem avaliações de impacto à proteção de dados, participação social e fiscalização ativa por parte da autoridade reguladora. Pedro Bastos Lobo Martins, por exemplo, complementa o debate ao destacar que o consentimento deve ser acompanhado de relatórios detalhados que

demonstrem a razoabilidade e a proporcionalidade do tratamento, especialmente para dados sensíveis e inferidos.

Martins (2019) reforça a importância da transparência e da responsabilização, alinhando-se às propostas de Bioni e Doneda, mas com um foco mais técnico nas avaliações de risco e no controle estatal. Essa convergência aponta para um consenso crescente na doutrina sobre a necessidade de um modelo pluralista e integrado de proteção, que supere as limitações do consentimento tradicional e assegure a proteção dos direitos fundamentais no ambiente digital.

Em síntese, as soluções apresentadas por esses autores oferecem um caminho para superar as críticas ao consentimento enquanto base legal única para o *profiling*, propondo um arcabouço regulatório que combine transparência, participação do titular, avaliação de impacto e regulação estatal ativa. Essas propostas dialogam diretamente com o objeto da pesquisa, que busca compreender e mitigar os impactos da perfilização no livre desenvolvimento da personalidade e na autodeterminação informativa dos usuários de redes sociais.

7 CONCLUSÃO

A presente dissertação investigou a compatibilidade da prática de *profiling*, adotada pelas redes sociais da Meta Platforms Inc., com os princípios do livre desenvolvimento da personalidade e da autodeterminação informativa, conforme previsto no artigo 2º da Lei Geral de Proteção de Dados (LGPD). Ao longo do trabalho, demonstrou-se a centralidade dos dados pessoais na economia da informação e os potenciais impactos da perfilização na formação da identidade dos usuários brasileiros. Considerando a expressiva adesão nacional às plataformas da empresa e os efeitos sistêmicos da coleta massiva de dados, esta conclusão tem por objetivo apresentar os principais resultados obtidos, refletir criticamente sobre os achados e apontar as contribuições da pesquisa ao campo jurídico.

O objetivo geral da pesquisa foi analisar se a técnica de *profiling*, aplicada no Facebook e no Instagram, é compatível com os princípios constitucionais do livre desenvolvimento da personalidade e da autodeterminação informativa. Para alcançar essa finalidade, foram definidos objetivos específicos, como mapear o arcabouço jurídico-normativo brasileiro sobre proteção de dados, avaliar a função e os limites do consentimento como base legal para a perfilização e investigar o modelo de negócios da Meta Platforms Inc.

A seleção das fontes e exemplos utilizados neste trabalho foi orientada por critérios de relevância temática, repercussão na mídia nacional, atualidade, reconhecimento acadêmico e acesso público. Foram priorizadas obras de referência na área de proteção de dados, privacidade, capitalismo de vigilância e sociologia. Como parâmetro jurídico foram utilizou se da Constituição Federal brasileira, as leis de proteção de dados brasileira e alemã (LGPD e GDPR), as legislações infraconstitucionais brasileiras afetas ao tema e decisões judiciais paradigmáticas que abriram os precedentes para a aplicação de direitos e deveres sobre o livre desenvolvimento da personalidade, com destaque para o julgamento da lei do censo alemão e o caso IBGE.

Ainda que a LGPD represente um marco normativo importante, sua estrutura atual não contempla com a devida profundidade os efeitos sistêmicos da perfilização. A ausência de mecanismos de transparência algorítmica, de prestação de contas e de participação social no controle dos dados processados por grandes plataformas dificulta a efetivação da proteção de dados como direito fundamental. Nesse sentido, este trabalho aponta a necessidade de revisão crítica da centralidade do consentimento e a adoção de mecanismos de regulação que reconheçam a natureza coletiva e política da proteção de dados.

Em relação a empresa Meta, distribui-se ao longo da pesquisa alguns casos de repercussão midiática que questionaram as atividades da empresa e levantaram discussões sobre a privacidade dos usuários e os limites de atuação dos aplicativos da Meta. Inc. A escolha dos exemplos buscou ilustrar situações emblemáticas e recentes, que envolvessem a empresa, ou outras empresas que possuem uma dinâmica de tratamento de dados similar, para a partir destes exemplos práticos aplicar a lógica dedutiva, conforme proposto na metodologia de pesquisa escolhida.

Também foram incluídas pesquisas empíricas sobre o uso de redes sociais no Brasil, a fim de agregar números sobre as críticas levantadas. Entretanto, sobre as pesquisas empíricas que foram juntadas, reconhece-se que a abordagem qualitativa e análise documental apresentam limitações à pesquisa, inerentes à natureza da fonte e disponibilidade de informações. A ausência de dados oficiais e acadêmicos sistematizados sobre práticas específicas de perfilização em redes sociais, especialmente no contexto brasileiro, impôs restrições à abrangência e à profundidade da análise.

A título de exemplo da observação feita no parágrafo anterior, ao tentar se averiguar o número médio de curtidas de usuários brasileiros no Facebook e Instagram (visto que as curtidas são normalmente citadas como uma métrica de mapeamento do gostos dos usuários), o texto recorreu a dados globais de 2018 fornecidos pela empresa *Brandwatch*, que além de não permitir uma validação com órgãos institucionais, apresenta uma defasagem temporal e a ausência de recorte geográfico mais preciso, o que somado à opacidade das plataformas prejudicou a exposição de resultados mais precisos sobre o real impacto da perfilização no livre desenvolvimento da personalidade.

A pesquisa demonstrou que a prática de *profiling*, ainda que formalmente amparada no consentimento do usuário, revela-se materialmente incompatível com os princípios do artigo 2º da LGPD. Na Seção 2 foi evidenciado que o ordenamento jurídico brasileiro reconhece os dados como direito fundamental de terceira geração, exigindo mecanismos de proteção coletiva. A Seção 3 aprofundou a relação entre identidade e dados, com destaque para a teoria da identidade narrativa de Paul Ricoeur, demonstrando como os algoritmos podem limitar a autodeterminação. Já na Seção 4, verificou-se que a economia informacional se estrutura na exploração de dados como ativos econômicos, o que impacta diretamente países como o Brasil, reforçando relações de dependência. A Seção 5 abordou os desafios globais da proteção de dados, com destaque para os riscos sociais da perfilização, e a Seção 6 apresentou

propostas regulatórias e a necessidade de revisão do papel do consentimento. Conclui-se que o atual modelo carece de uma regulação mais eficaz e protetiva

No que se refere aos objetivos propostos o trabalho cumpriu com as finalidades às quais se propôs visto que: (i) analisou o consentimento sob a ótica da LGPD e da doutrina brasileira; (ii) investigou o modelo de negócio da Meta Inc. com ênfase na prática de perfilização; (iii) avaliou a suficiência das bases legais atualmente utilizadas, como o consentimento e o legítimo interesse; e (iv) propôs alternativas normativas e regulatórias voltadas à proteção dos titulares em um ambiente digital opaco e assimétrico.

Este trabalho se propôs a ultrapassar a abordagem tradicional, centrada na legalidade abstrata e formal do consentimento, ao investigar sua materialidade no ambiente específico das redes sociais. A partir dos resultados encontrados, a pesquisa sugeriu que a questão seja analisada sob a perspectiva de um direito coletivo, necessitando da interferência do Estado, entendendo que a hipossuficiência técnica impossibilita uma relação equilibrada entre plataformas digitais e consumidores.

Ao invés de restringir o estudo da perfilização aos seus efeitos individuais, este trabalho se dedicou a analisar os impactos difusos e sistêmicos da prática, bem como levou em consideração a diferença procedural entre a perfilização tradicional, e a perfilização feitas nas redes sociais, onde a finalidade do tratamento é pensada a partir da formação do perfil, não existindo de maneira prévia a captação de dados.

Sob a perspectiva de uma continuidade acadêmica o estudo pode ser utilizado como uma base teórica para a discussão da perfilização em contextos sem objetivo específico, que operam com a inversão das etapas de finalidade > captação de dados > Tratamento > decisão, a exemplo das redes sociais que operam na lógica Captação de dados > tratamento > Finalidade. Sugere se também investigação empírica sobre os efeitos concretos da perfilização em diferentes grupos sociais, especialmente usuários em condição de vulnerabilidade digital.

Em síntese, o presente estudo evidenciou que a perfilização algorítmica praticada pelas redes sociais da Meta Platforms Inc. representa um desafio substancial à proteção dos direitos fundamentais no ambiente digital. Ainda que a LGPD, em conjuntos com outros institutos, forneça uma base normativa relevante, sua efetividade depende da superação de uma abordagem individualista e da adoção de políticas públicas regulatórias que aprofundem na discussão sobre os impactos coletivos do uso de dados pessoais.

Verificou se ainda que ao tratar dados como ativos econômicos e os usuários como fontes de extração, o modelo atual reitera desigualdades estruturais, e que a ausência de

limites mais específicos sobre perfilização abre espaço para arbitrariedades, incompatíveis com a dignidade humana. Resta à comunidade jurídica, ao legislador e à sociedade civil refletirem coletivamente sobre os limites da atuação das *big techs* e a necessidade de uma regulação que esteja à altura da complexidade da economia digital.

Enquanto isso, seguimos clicando em "li e concordo".

REFERÊNCIAS

ACCIOLY FILHO, Lauro. **A Batalha Tecnológica entre Estados Unidos e China**. Le Monde Diplomatique Brasil, 2025. Disponível em: <https://diplomatique.org.br/a-batalha-tecnologica-entre-estados-unidos-e-china/>. Acesso em: 21 jun. 2025.

AGUIAR, Daniel Stochero de. **Estudo de caso da Cambridge Analytica na eleição**. 2021. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade de Caxias do Sul, Caxias do Sul, 2021. Disponível em: <https://repositorio.ucs.br/xmlui/bitstream/handle/11338/8976/TCC%20Daniel%20Stochero%20de%20Aguiar.pdf?sequence=1&isAllowed=y>. Acesso em: 04 jul. 2025.

ALEMANHA. **Lei Fundamental da República Federal da Alemanha**. Trad. Aachen Assis Mendonça. Berlim: Parlamento Federal Alemão, 1949. Disponível em: <https://www.btg-bestellservice.de/pdf/80208000.pdf>. Acesso em: 16 de maio de 2025.

ALMADA, Marco. **Revisão humana de decisões automatizadas**. Pós Debate. 2019. Disponível em: https://www.academia.edu/41483884/Revis%C3%A3o_humana_de_decis%C3%B5es_automatizadas. Acesso em: 15 jul. 2025.

ALTMAN, Irwin. **The environment and social behavior: privacy, personal space, territory, crowding**. Brooks/Cole Pub, 1975.

ANGWIN, Julia *et al.* **Machine Bias**: There's software used across the country to predict future criminals. And it's biased against blacks. ProPublica, 2016. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. Acesso em: 15 jul. 2025.

ANPD. **Nota Técnica nº 12/2025**. Brasil, 2025. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/notas-tecnicas/nota-tecnica-no-12-2025-con1-cgn-anpd>. Acesso em: 20 jun. 2025.

ANPD. **Relatório de Análise de Impacto Regulatório**: Dosimetria das Sanções Administrativas. Brasília, 2022. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/2022-06-30_air_reg_dosimetria_.pdf. Acesso em: 20 abr. 2025.

ANPD. **Estudo Técnico a Anonimização de Dados na LGPD**: Análise Jurídica. Brasilia, 2023. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/estudo_tecnico_sobre_anonimizacao_de_dados_na_lgpd_analise_juridica.pdf. Acesso em: 20 abr. 2025.

ANPD. **Webinário**: Tomada de Subsídios sobre Tratamento Automatizado de Dados Pessoais. YouTube, 15 maio 2025. Disponível em: <https://www.youtube.com/watch?v=SyrYFzmMu4g>. Acesso em: 07 jul. 2025.

ARRUDA, Vinícius Cervantes Gorgone. **Big data, dados pessoais e propriedade intelectual: limites e tutela jurídica das bases de dados**. 2. ed. Curitiba: CRV, 2021. 318 p. ISBN 978-65-251-1144-5.

AVELINO, Rodolfo. Imperialismo de plataforma, Colonialismo digital: dimensões da colonialidade nas grandes plataformas. In: CASSINO, João Francisco; SOUZA, Joyce;

SILVEIRA, Sérgio Amadeu da (Orgs.). **Colonialismo de dados e modulação algorítmica: tecnopolítica, sujeição e guerra neoliberal**. São Paulo: Autonomia Literária, 2021. p.67-83.

AYRES PINTO, Danielle Jacon; MORAES, Isabela. As mídias digitais como ferramentas de manipulação de processos eleitorais democráticos: uma análise do caso Brexit. **Revista de Estudios Sociales**, n. 74, 2020, out./dez., p. 71-82. Disponível em: <https://www.redalyc.org/articulo.oa?id=81564846006>. Acesso em: 04 jul. 2025.

BAKSHY, Eytan; MESSING, Solomon; ADAMIC, Lada A. Political science. Exposure to ideologically diverse news and opinion on Facebook. **Science**, v. 348, n. 6239, p. 1130–1132, 2015. DOI: <https://doi.org/10.1126/science.aaa1160>.

BARROSO, Luís Roberto. **Interpretação e aplicação da Constituição**: fundamentos de uma dogmática constitucional transformadora. 7. ed. São Paulo: Saraiva, 2018.

BASTOS, Celso Ribeiro; MARTINS, Ives Gandra da Silva. **Comentários à Constituição do Brasil**: (promulgada em 5 de outubro de 1988). 2. ed. São Paulo: Saraiva, 2001.

BAUMAN, Zygmunt. **Vigilância líquida**. Rio de Janeiro: Zahar, 2013.

BBC NEWS Brasil. **Como o Facebook mudou a internet, o comércio e até a política. 2021**. Disponível em: <https://www.bbc.com/portuguese/internacional-55966587>. Acesso em: 21 jun. 2025.

BBC News Brasil. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades**. BBC, 20 mar. 2018. Disponível em: <https://www.bbc.com/portuguese/internacional-43461751>. Acesso em: 21 abr. 2025.

BBC NEWS. **Cambridge Analytica**: The story sofar. BBC News, Londres, 20 mar. 2018. Disponível em: <https://www.bbc.com/news/technology-43465968>. Acesso em: 15 jul. 2025.

BONI, Bruno Ricardo (Org.). **Proteção de dados**: contexto, narrativas e elementos fundantes. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021.

BONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BONI, Bruno; MARTINS, Pedro. **Devido processo informacional: um salto teórico-dogmático necessário?** 2020. Disponível em: <https://brunoboni.com.br/wp-content/uploads/2020/08/Ensaio-Devido-Processo-Informacional1.pdf>. Acesso em: 7 jul. 2025

BORGES, Roxana Cardoso Brasileiro. O Código Civil e o direito da personalidade. **Revista do CEPEJ**, Salvador, n. 6, p. 37-56, 2020. Disponível em: <https://periodicos.ufba.br/index.php/CEPEJ/article/download/37603/21456/135222>. Acesso em: Acesso em: 2 jun. 2025.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988: atualizada até a Emenda Constitucional nº 20, de 15 de dezembro de dezembro de 1988. 21.ed. São Paulo: Saraiva, 1999.

BRASIL. **Lei nº 8.078**, de 11 de setembro de 1990. Código de Defesa do Consumidor. Brasil, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm. Acesso em: 22 de abr. 2024.

BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasil, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 12 jun. 2024.

BRASIL. **Lei n. 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 jun. 2024.

BRASIL. **Medida provisória n. 954**, de 17 de abril de 2020. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Brasília, 2020. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 16 de maio de 2025.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.316.921 - RJ** (2011/0307909-6). Relatora: Ministra Nancy Andrighi, 26 de junho de 2012. Disponível em: <https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=23036667&tipo=5&nreg=20110307909&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20120629&formato=PDF&salvar=f>. Acesso em: 2 jun. 2025.

BRASIL. Supremo Tribunal Federal. **ADI nº 6.387**. Medida Cautelar em Ação Direta de inconstitucionalidade. Reqte: CFOAB. Relatora: Min. Rosa Weber., 07 mai. 2020. Acesso em: 20 jun. 2025. Disponível em: <https://www.stf.jus.br/arquivo/cms/bibliotecaConsulta ProdutoBibliotecaPastaFachin/anexo/ADI6387MCREF.pdf>. Acesso em: 23 fev. 2025.

BRASIL. Supremo Tribunal Federal (2. Turma). **Recurso Extraordinário n. 201.819-8**. Relator: Min. Sepúlveda Pertence, 10 de outubro de 2005. Brasília, 2005. Disponível em: Jusbrasil. Acesso em: 7 jul. 2025

BRASIL. Supremo Tribunal Federal. **RE 1.037.396 (Tema 987) e 1.057.258 (Tema 533)**: Responsabilidade de plataformas digitais por conteúdo de terceiros. Brasília, 2025. Disponível em: <https://noticias.stf.jus.br/postsnoticias/stf-define-parametros-para-responsabilizacao-de-plataformas-por-conteudos-de-terceiros/>. Acesso em: 9 jul. 2025.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. **Revealed**: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian, 17 mar.

2018. Disponível em: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>. Acesso em: 10 jul. 2025.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2630/2020**. Brasília, 2024. Disponível em: <https://www.camara.leg.br/propostas-legislativas/2247670>. Acesso em: 8 jul. 2025.

CANCELIER, Mikhail Vieira de Lorenzi. **Infinito Particular: privacidade no Século XXI e a Manutenção do Direito de Estar Só**. 2016. Tese (Doutorado em Direito) – Universidade Federal de Santa Catarina, Florianópolis, 2016. Disponível em: <https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/174424/PDPC1275-T.pdf?sequence=1&isAllowed=y>. Acesso em: 30 mar. 2025.

CARDOSO BRASILEIRO BORGES, R. O Código Civil e o Direito da Personalidade. **Revista do CEPEJ**, n. 11, 2020. Disponível em: <https://periodicos.ufba.br/index.php/CEPEJ/article/view/37603>. Acesso em: 29 maio. 2025.

CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da (Orgs.). **Colonialismo de dados e modulação algorítmica: tecnopolítica, sujeição e guerra neoliberal**. São Paulo: Autonomia Literária, 2021.

CASTELLS, Manuel. A sociedade em rede. São Paulo: Paz e Terra, 1999.

CASTELLS, Manuel. **Fim de milênio** [recurso eletrônico]. Traduzido por Klaus Brandini Gerhardt, Roneide Venancio Majer. 1. ed. São Paulo: Paz e Terra, 2020.

CASTRO, Cynthia Dias de. **Propaganda enganosa e abusiva: publicidade, marketing e digital influencer**. Trabalho de Conclusão de Curso – Pontifícia Universidade Católica de Goiás, Escola de Direito, Negócios e Comunicação, Goiânia, 2023. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/6012/1/TCC%20-20CYNTHIA%20DIAS%20DE%20CASTRO.pdf>. Acesso em: 30 mar. 2025.

CEDIS-IDP. **O papel da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) conforme a nova Lei Geral de Proteção de Dados Pessoais (LGPD)**. 2020. Disponível em: <https://wpcdn.idp.edu.br/idpsiteportal/2020/05/PT-CIPL-IDP-Paper-on-the-Role-of-the-ANPD-under-the-LGPD-04.17.2020.pdf>. Acesso em: 20 abr. 2025.

CHAGAS, D. M. F.; GOMES, S. M.; MARTINS, A. F. Impacto das mídias digitais na saúde mental de adolescentes: um estudo sobre depressão e estresse. **Id Online - Revista Multidisciplinar e de Psicologia**, v. 14, n. 51, p. 1-20, 2025. Disponível em: <https://idonline.emnuvens.com.br/id/article/view/4161>. Acesso em: 14 set. 2025.

CITRON, Danielle Keats; PASQUALE, Frank. The Scored Society: due process for automated predictions. **Washington Law Review**, v. 89, 2014. Disponível em: <https://digitalcommons.law.uw.edu/wlr/vol89/iss1/2/>. Acesso em: 10 abr. 2025.

CRUZ, Leonardo Ribeiro da; SARAIVA, Filipe de Oliveira; AMIEL, Tel. **Coletando dados sobre o Capitalismo de Vigilância nas instituições públicas do ensino superior do Brasil**. In: SIMPÓSIO LAVITS, 6., 2019, Salvador. Disponível em: https://lavits.org/wp-content/uploads/2019/12/Cruz_Saraiva_Amiel-2019-LAVITS-1.pdf. Acesso em: 21 jun. 2025.

DATAPORTAL; KEPÍOS. *Digital 2025: Brazil — DataReportal Local Country Headlines / Global Digital Insights*. [S.l.], janeiro de 2025. Disponível em:

<https://datareportal.com/reports/digital-2025-brazil>. Acesso em: 20 de setembro. 2025.

DONEDA, Danilo. A proteção de dados pessoais e a pandemia da COVID-19. **Revista de Direito Civil Contemporâneo**, São Paulo, n. 23, p. 17-33, 2020. Disponível em: <https://www.revistadireitocivil.com.br/edicoes>. Acesso em: 16 jul. 2025.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da autoridade da proteção de dados. Rio de Janeiro: Renovar, 2006.

FACHIN, Luiz Edson. Análise crítica, construtiva e de índole constitucional da disciplina dos direitos da personalidade no Código Civil brasileiro: fundamentos, limites e transmissibilidade. **Revista Jurídica**, v. 362, 2007. Disponível em: <https://www.abdireitocivil.com.br/wp-content/uploads/2013/07/An%C3%A1lise-Cr%C3%ADtica-Construtiva-e-de-%C3%8Dndole-Constitucional-da-Disciplina-dos-Direitos-da-Personalidade-no-C%C3%B3digo-Civil-Brasileiro-Fundamentos-Limites-e-Transmissibilidade.pdf>. Acesso em: 22 mar. 2025.

FILIPPO, Thiago Baldani Gomes de. Direitos da personalidade e dignidade da pessoa humana: aproximações e distinções. **Revista da Escola Paulista da Magistratura**, São Paulo, v. 1, n. 1, p. 39-70, 2009. Disponível em: <https://epm.tjsp.jus.br/Artigo/Acervo/2927?pagina=39>. Acesso em: 27 maio 2025.

FM2S. **Meta platforms**: história, aquisições e futuro. 2024. Disponível em: <https://www.fm2s.com.br/blog/meta-platforms>. Acesso em: 26 abr. 2025.

FACEBOOK admite que dados de brasileiros foram usados pela Cambridge Analytica. **Folha de S. Paulo**, São Paulo, 4 abr. 2018. Disponível em: <https://www1.folha.uol.com.br/mercado/2018/04/facebook-admite-que-dados-de-brasileiros-foram-usados-pela-cambridge-analytica.shtml>. Acesso em: 15 jul. 2025.

FORNASIER, Mateus de Oliveira; BECK, Cesar. Cambridge Analytica: escândalo, legado e possíveis futuros para a democracia. **Revista do Departamento de Ciências Jurídicas e Sociais da Unijuí**, v. 29, n. 53, p. 182-195, jan./jun. 2020. Disponível em: <https://www.revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/10033/6360>. Acesso em: 04 jul. 2025.

GAMA, Rafaela. Apagão de informações: plataformas digitais têm baixa transparência de dados e publicidade no Brasil, aponta estudo. **O Globo**, 2024. Disponível em: <https://oglobo.globo.com/blogs/sonar-a-escuta-das-redes/post/2024/11/apagao-de-informacoes-plataformas-digitais-tem-baixa-transparencia-de-dados-e-publicidade-no-brasil-aponta-estudo.ghtml>. Acesso em: 30 mar. 2025.

GDPR DIGEST. **Definições**. 2025. Disponível em: <https://gdprdigest.com/pt-pt/pt-pt-article-4>. Acesso em: 23 abr. 2025

GHOSH, Shona. Facebook knows you better than your spouse does. Campaign, 2015. Disponível em: <https://www.campaignlive.com/article/facebook-knows-better-spouse-does/1329114>. Acesso em: 31 maio 2025.

GONÇALVES, Beatriz. **Pesquisa Instagram no Brasil**: dados que revelam as preferências dos usuários na rede social. Opinion Box, 2024. Disponível em: <https://blog.opinionbox.com/pesquisa-instagram/>. Acesso em: 22 abr. 2025.

IEDI. **Complexidade Econômica**: Brasil e o Mundo. São Paulo, 2024. Disponível em: https://iedi.org.br/cartas/carta_iedi_n_1245.html. Acesso em: 2 jul. 2025.

INICIATIVA EDUCAÇÃO ABERTA. **Sobre**. Observatório Educação Vigiada, [2025]. Disponível em: <https://educacaovigiada.org.br/pt/sobre.html>. Acesso em: 21 jun. 2025.

KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior. **Proceedings of the National Academy of Sciences**, Washington, v. 110, n. 15, p. 5802-5805, 2013. Disponível em: <https://doi.org/10.1073/pnas.1218772110>. Acesso em: 6 abr. 2025.

KRAMER, Adam D. I.; GUILLORY, Jamie E.; HANCOCK, Jeffrey T. Experimental evidence of massive-scale emotional contagion through social networks. **PNAS**, v. 111, n. 29, p. 8788-8790, July 2014. Disponível em: <http://www.pnas.org/content/111/29/8788.full.pdf>. Acesso em: 3 ago. 2025.

LIMA, Catarina Carneiro de Andrade; NOGUEIRA, Silas. **Redes sociais da internet: Identidade, pertencimento e sociabilidade**. In: Ciências da Comunicação 3. Atena Editora, 2023. Disponível em: <https://atenaeditora.com.br/internet-identidade-pertencimento>. Acesso em: 27 abr. 2025.

LIRA, Ariana Galhardi et al. Uso de redes sociais, influência da mídia e insatisfação com a imagem corporal de adolescentes brasileiras. **Revista Brasileira de Psiquiatria**, Rio de Janeiro, v. 66, n. 3, p. 201–209, jul./set. 2017. Disponível em: <http://dx.doi.org/10.1590/0047-2085.000000166>. Acesso em: 16 jul. 2025.

LOMAS, Natasha. **Facebook faces fresh criticism over ad targeting of sensitive interests**. TechCrunch, 2018. Disponível em: <https://techcrunch.com/2018/05/16/facebook-faces-fresh-criticism-over-ad-targeting-of-sensitive-interests/>. Acesso em: 19/04/2025.

MACHADO, Almir de Melo. Psicologia social e redes sociais: impactos no comportamento e bem-estar. **Revista Científica IPEDSS**, v. 4, n. 2, p. 1-27, 15 out. 2024. Disponível em: <https://www.revistacientificaipedss.com/psicologia-social-e-redes-sociais-impactos-no-comportamento-e-bem-estar>. Acesso em: 24 abr. 2025.

MACHADO, Débora Franco. A colonização dos dados como produto das operações das mídias sociais no Sul Global. In: SILVEIRA, Sergio Amadeu da; SOUZA, Jorge; CASSINO, João Francisco. **Colonialismo de dados**: como opera a trincheira algorítmica na Guerra Neoliberal. São Paulo: Autonomia Literária, 2021. Disponível em: https://fpabramo.org.br/editora/wp-content/uploads/sites/17/2022/06/colonialismodedados_fpa_WEB.pdf. Acesso em: 15 fev. 2025.

MARQUES, Cláudia Lima (Coord.). **Estudos sobre a proteção do consumidor no Brasil e no MERCOSUL**. Porto Alegre: Livraria do Advogado, Instituto Brasileiro de Política e Direito do Consumidor, 1994.

MARTINS, Leonardo. **Tribunal Constitucional Federal Alemão**: decisões anotadas sobre direitos fundamentais. São Paulo: Konrad-Adenauer Stiftung, 2016.

MARTINS, Pedro Bastos Lobo. **Dados pessoais sensíveis e inferências**. DTIBR, 2019. Disponível em: <https://www.dtibr.com/post/dados-pessoais>. Acesso em: 21 abr. 2025

MAXIMILIANO, Carlos. **Hermenêutica e aplicação do direito**. Rio de Janeiro: Editora Forense, 2006.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Pensar Revista de Ciências Jurídicas**, Fortaleza, v. 25, n. 4, p. 1–18, out./dez. 2020. Disponível em: <https://ojs.unifor.br/rpen/article/download/10828/pdf/44878>. Acesso em: 16 maio 2025.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental [e-book]. São Paulo: Saraiva, 2014. Série IDP: Linha Pesquisa Acadêmica.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: fundamentos da regulamentação. **Revista de Direito do Consumidor**, São Paulo, v. 105, p. 89-116, 2015.

META PLATFORMS. **Termos de Serviço do Facebook**. 2025. Disponível em: <https://www.facebook.com/legal/terms>. Acesso em: 2 jul. 2025

MIAN, Mariella Batarra. Universidades federais brasileiras a serviço da lógica colonial de exploração de dados. In: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da (Orgs.). Colonialismo de dados e modulação algorítmica: tecnopolítica, sujeição e guerra neoliberal. São Paulo: Autonomia Literária, 2022.

MONTARDO, S. P. F.; et al. Filtros embelezadores no Instagram Stories: pistas iniciais sobre a plataformaização da beleza. **Logos**, v. 28, n. 2, p. 29-40, 2021. Disponível em: <https://www.e-publicacoes.uerj.br/logos/article/view/60900>. Acesso em: 14 set. 2025.

MONTEIRO, Gustavo Testa. O controle de constitucionalidade da MP 954/2020 e o direito à proteção de dados pessoais no Brasil. **Revista Brasileira de Direito**, Passo Fundo, v. 16, n. 2, p. 88-107, 2020. Disponível em: <https://seer.imed.edu.br/index.php/revistadeldireito/article/view/4414>. Acesso em: 16 jul. 2025.

O FACEBOOK é inovador? Exame, 2011. Disponível em: <https://exame.com/colunistas/innovacao-na-pratica/o-facebook-e-inovador/>. Acesso em: 26 abr. 2025.

PACETE, Luiz Gustavo. **Brasil é o terceiro país que mais consome redes sociais em todo o mundo**. Forbes, 2023. Disponível em: <https://forbes.com.br/forbes-tech/2023/03/brasil-e-o-terceiro-pais-que-mais-consome-redes-sociais-em-todo-o-mundo/>. Acesso em: 22 abr. 2025.

PALMEIRA, Carlos. **Facebook agora é Meta**: o que há por trás da mudança de nome? TecMundo, 2021. Disponível em: <https://www.tecmundo.com.br/mercado/227791-ha-tras-mudanca-nome-facebook-meta.htm>. Acesso em: 26 abr. 2025.

PEREIRA, João Vitor Nunes; PONTES, Ritiele Queles; TOZATTO, Alessandra. A influência das redes sociais no processo de construção da identidade. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 8, n. 10, p. 591-604, out. 2022. Disponível em: <https://periodicorease.pro.br/rease/article/view/7105/2771>. Acesso em: 27 abr. 2025.

PINTO, Paulo Mota. O direito geral de personalidade e os direitos de personalidade. **Revista do Supremo Tribunal de Justiça**, Lisboa, n. 5, p. 13, 2024. Disponível em: <https://catalogobib.parlamento.pt:82/plp/pn-tl/winlibsrch.aspx?skey=C9A908D74E0C40E7A6E30740F249BC60&cap=&pesq=5&thes1=25761&dtype=lista&prn=true&doc=204343>. Acesso em: 10 abr. 2025.

POECHHACKER, Nikolaus; NYCKEL, Eva-Maria. Logistics of Probability: Anticipatory Shipping and the Production of Markets. In: BURKHARDT, Marcus; SHNAYIEN, Mary; GRASHÖFER, Katja (Org.). **Explorations in Digital Cultures**. Lüneburg: mesonpress, 2020. Disponível em: <https://mediarep.org/server/api/core/bitstreams/1a66205f-4b76-4392-b46c-1db25b942bc2/content>. Acesso em: 11 maio 2025.

REALE, Miguel. **O estado democrático de direito e o conflito das ideologias**. 3. ed., rev. São Paulo: Saraiva, 2010

REZENDE, Patrick. Influenciadores digitais e subjetivação: o poder algorítmico nas redes sociais digitais. **Revista de Pós-Graduação em Ciências Sociais da UFES**, Vitória, v. 10, n. 25, p. 144–162, out. 2020. Disponível em: <https://periodicos.ufes.br/percursos/article/view/30680/21747>. Acesso em: 16 jul. 2025.

RICOEUR, Paul. O si mesmo como um outro. Tradução de Lucy Moreira Cesar. Campinas: Papirus, 1991.

RIGHI, H. M.; SANTOS, D. F. L.; OLIVEIRA, L. G. Dados como commodities: dependência tecnológica e economia informacional. **Revista de Economia Contemporânea**, v. 25, n. 1, 2021.

RODRIGUES, Jonatan. **95 estatísticas de Redes Sociais para conhecer em 2024**. RD Station, 2024. Disponível em: <https://www.rdstation.com/blog/marketing/estatisticas-redes-sociais/>. Acesso em: 27 abr. 2025.

ROSENBERG, Matthew; CONFESSORE, Nicholas; CADWALLADR, Carole. How Trump Consultants Exploited the Facebook Data of Millions. **The New York Times**, New York, 17 mar. 2018. Disponível em: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump.html>. Acesso em: 15 jul. 2025.

ROSSI, Carla. **Os desafios envolvendo regulação e inovação tecnológica.** Época Negócios, 2023. Disponível em: <https://epocanegocios.globo.com/regulacao-e-inovacao-tecnologica.ghml>. Acesso em: 23 abr. 2025.

ROUVROY, Antoinette. O Fim da Crítica: Behaviorismo de Dados Versus Devido Processo. In: HILDEBRANDT, Mireille; DE VRIES, Katja (Org.). Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology. **Abingdon, Oxon;** New York, NY: Routledge, 2013. cap. 6, p. 143-167.

SANTANA, R. D.; NEVES, B. C. Entre filtros e bolhas: a modulação algorítmica na sociedade pós-panóptica. Logeion: **Filosofia da Informação**, Rio de Janeiro, v. 8, n. 2, p. 47-64, mar./ago. 2022. Disponível em: <https://revista.ibict.br/fiinf/article/view/5825/5529>. Acesso em: 1 jul. 2025.

SARMENTO, Daniel. **A ponderação de princípios como técnica decisória no direito constitucional.** Rio de Janeiro: Lumen Juris, 2007.

SARMENTO, Daniel. **Direitos fundamentais e Relações privadas.** Rio de Janeiro: Lumen Juris, 2004.

SENATO DA REPÚBLICA ITALIANA. **Constituição da República Italiana** (tradução em língua portuguesa). Roma: Senado da República, 2023. Disponível em: https://www.senato.it/sites/default/files/media/documents/Costituzione_PORTOGHESE.pdf. Acesso em: 30 maio 2025.

SILVA, G. F.; SILVA, J. S. Manipulação algorítmica: filtros bolhas e o impacto da IA na desinformação. In: CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO, 47., 2024, Porto Alegre. **Anais** [...]. Porto Alegre: Intercom, 2024. Disponível em: <https://sistemas.intercom.org.br/pdf/submissao/nacional/17/06282024182222667f298e30924.pdf>. Acesso em: 1 jul. 2025.

SILVA, Gutavo Henrique Luz *et al.* A Year in Privacy: Transferências Internacionais de Dados. **Revisão técnica:** Fernando Bousso. São Paulo: Baptista Luz Advogados, 2022. Disponível em: https://baptistaluz.com.br/wp-content/uploads/2022/12/AYIP_12_V2.pdf. Acesso em: 20 abr. 2025.

SILVA, João Paulo Borges da. O caso Cambridge Analytica e a sociedade de risco: reflexões sobre o compartilhamento indevido de dados pessoais. **Revista Themis**, v. 18, n. 2, p. 209-232, 2021. Disponível em: <https://revistathemis.tjce.jus.br/THEMIS/article/download/1050/785/3901>. Acesso em: 04 jul. 2025.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo.** 42. ed. rev. e atual. São Paulo: Malheiros Editores, 2019.

SILVA, Luciana Ferreira da; SANTOS, Pedro Otto Souza; JESUS, Tâmara Silene Moura de. Novos contornos do direito à privacidade: profiling e a proteção de dados pessoais. **Brazilian Journal of Development**, v. 7, n. 11, 2021. Disponível em: <https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/39356> Acesso em: 7 abr. 2025.

SILVA, Samara Monayari Magalhães; DINALLO, Andressa Rangel. A origem e a evolução dos direitos da personalidade e a sua tutela no ordenamento jurídico brasileiro. *Brazilian Journal of Development*, Curitiba, v. 7, n. 7, p. 70355-70368, jul. 2021. DOI: 10.34117/bjdv7n7-286.

SILVEIRA, Sérgio Amadeu da. **Tudo sobre tod@s**: redes digitais, privacidade e venda de dados pessoais. 1. ed. São Paulo: Edições Sesc SP, 2017.

SKINNER, B. F. **Science and human behavior**. New York: Macmillan, 1953.

SMITH, Kit. **53 Incredible Facebook Statisticsand Facts**. Brandwatch, 2019. Disponível em: <https://www.brandwatch.com/blog/facebook-statistics/>. Acesso em: 2 jun. 2025.

SOBRINHO, Asdrúbal Borges Formiga; BARBOSA, Alexandre Mota. Criatividade no Instagram como ferramenta de inovação para as organizações. **Signos do Consumo**, São Paulo, v. 6, n. 1, p. 125-137, jul. 2014. Disponível em: <https://www.revistas.usp.br/signosdoconsumo/article/download/101406/100020/177000>. Acesso em: 26 abr. 2025

SOLOVE, Daniel J. **Understanding Privacy**. Cambridge: Harvard University Press, 2008.

STANCIOLI, Brunello. **Renúncia ao exercício dos direitos da personalidade ou como alguém se torna o que quiser**. Belo Horizonte: Del Rey, 2011.

SUSANTO, Azhar; MEIRYANI. **System development method with the prototype method**. *International Journal of Scientific & Technology Research*, v. 8, n. 7, p. 141-144, July 2019. Disponível em: <https://ijstr.org/final-print/july2019/System-Development-Method-With-The-Prototype-Method.pdf>. Acesso em: 14 set. 2025

SWISHER , Kara, Dot-Com Bubble Has Burst; Will Things Worsen in 2001? **The Wall Street Journal**, 2000. Disponível em: <http://www.wsj.com/articles/SB97709118336535099>. Acesso em: 21 jun. 2025.

TELES, Ariel Soares. **Um Mecanismo Baseado em Lógica Nebulosa para a Identificação de Situações de Usuários Aplicado à Privacidade em Redes Sociais Móveis**. 2017. 170 f. Tese (Doutorado em Engenharia de Eletricidade) – Centro de Ciências Exatas e Tecnologia, Universidade Federal do Maranhão, São Luís, 2017. Disponível em: <https://tedebc.ufma.br/jspui/handle/tede/1250>. Acesso em: 11 maio 2025.

TEÓFILO, Caroline; CABELLA, Daniela M. Monte Serrat. **Schrems II e LGPD**: reflexões acerca dos impactos da decisão da CJEU no cenário brasileiro. *Migalhas*, 13 ago. 2020. Disponível em: <https://www.migalhas.com.br/depeso/331982/schrems-ii-e-lgpd--reflexoes-acerca-dos-impactos-da-decisao-da-cjeu-no-cenario-brasileiro>. Acesso em: 20 abr. 2025.

THE WORLD'S most valuable resource is no longer oil, but data. *The Economist*, 2017. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 22 abr. 2025.

TIGRE, Paulo Bastos. Paradigmas Tecnológicos e Teorias Econômicas da Firma. **Revista de Economia Contemporânea**, UFRJ, versão preliminar publicada em 1998. fevereiro de 2005. Disponível em: https://www5.pucsp.br/eitt/downloads/III_Ciclo_Art_Paulo_Tigre_Paradigmas_Tecnologicos_e_Teorias_.pdf. Acesso em: 10 jan. 2025.

TUMELERO, Naína Ariana Souza. **Perfilização e coleta de dados comportamentais: as políticas de privacidade da Google pela ótica consumerista no capitalismo da vigilância.** *Revista de Direito, Globalização e Responsabilidade nas Relações de Consumo*, v. 7, n. 1, p. 55–74, jan./jul. 2021. Disponível em: indexlaw.org. Acesso em: 20 set. 2025.

UNAERP. **Emenda Constitucional nº 115/2022 e a proteção de dados pessoais como direito fundamental.** Ribeirão Preto: Universidade de Ribeirão Preto, 2024. Disponível em: <https://www.unaerp.br/>. Acesso em: 14 set. 2025.

Revista de Direito, Globalização e Responsabilidade nas Relações de Consumo, v. 7, n. 1, p. 55-74, jan./jul. 2021. Disponível em: <https://www.indexlaw.org/index.php/revistadgrc/article/download/7771/pdf>. Acesso em: 18 abr. 2025.

VERÍSSIMO, Isabela. Brasil dispara como um dos maiores consumidores de mídias sociais, segundo pesquisa. **Jornal Digital Recife**, 2024. Disponível em: <https://jornaldigital.recife.br/2024/04/10/brasil-dispara-como-um-dos-maiores-consumidores-de-mídias-sociais-segundo-pesquisa/>. Acesso em: 27 abr. 2025.

WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking Data Protection Law in the Age of Big Data and AI. **Columbia Business Law Review**, Nova Iorque, v. 2019, n. 2, p. 1-130, 2019, p. 87. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829. Acesso em; 10 jan. 2025.

WARREN, Samuel D.; BRANDEIS, Louis D.. The right to privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, 1890. Disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 15 jun. 2025.

ZAJONC, Robert B. Attitudinal effects of mere exposure. **Journal of Personality and Social Psychology Monograph Supplement**, v. 9, n. 2, jun. 1968. Disponível em: https://www.psy.lmu.de/allg2/download/audriemmo/ws1011/mere_exposure_effect.pdf. Acesso em: 16 jul. 2025.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância:** a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2019.